سلسلة كتب المستقبل

البلوكتشين

أنترنت الأشياء

الذكاء الاصطناعي

مجتمع ما بعد المعلومات

تأثير الثورة الصناعية الرابعة على الأمن القومي

إيهاب خليفة





مجتمع ما بعد المعلومات

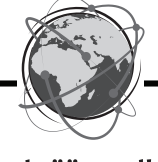
إيهاب خليفة

مُجتمع ما بعد المعلومات

تأثير الثورة الصناعية الرابعة على الأمن القومي

إيهاب خليفة





المستقبل
للأبحاث والدراسات المتقدمة

مُجتمع ما بعد المعلومات

إيهاب خليفة

الطبعة الأولى: 2019

رقم الإيداع: 2019/4023

الترقيم الدولي: **978977319484**

الغلاف: عبدالله خميس

مراجعة لغوية: محمد بكر حامد

60 شارع قصر العيني - 11451 - القاهرة

ت: 27921943 - 27954529 فاكس: 27947566

www.alarabipublishing.com.eg



بطاقة فهرسة

خليفة، إيهاب

مُجتمع ما بعد المعلومات/ إيهاب خليفة، القاهرة: العربي للنشر والتوزيع، 2019 - ص؛سم

تدمك: **978977319484**

1- ثورة المعلومات – الجوانب الاجتماعية

أ- العنوان 306.42



عن المستقبل:

مركز تفكير (Think Tank) مستقل، أنشئ عام 2014، في أبوظبي، بدولة الإمارات العربية المتحدة، للمساهمة في تعميق الحوار العام، ومساندة صنع القرار، ودعم البحث العلمي، فيما يتعلق باتجاهات المستقبل، التي أصبحت تمثل إشكالية حقيقية بالمنطقة، في ظل حالة عدم الاستقرار وعدم القدرة على التنبؤ، خلال المرحلة الحالية، من خلال رصد وتحليل وتقدير «المستجدات» المتعلقة بالتحولات السياسية والاتجاهات الأمنية، والتوجهات الاقتصادية والتطورات التكنولوجية، والتفاعلات المجتمعية والثقافية، المؤثرة على مستقبل منطقة الخليج، وفي نطاق الشرق الأوسط عموماً.

للاتصال والمعلومات:
البرج الدولي، شارع الكرامة، منطقة مركز المعارض، الطابق (24)
ص.ب 111414 أبوظبي, الإمارات العربية المتحدة
هاتف: 24444513-971+, فاكس: 24444732-971+
العلاقات العامة: 999 657 502 971+
Email: info@futureuae.com
www.futureuae.com

الفهرس

مُقدِّمة:

العالمُ على أعتاب ثورة نوعيَّة جديدة يقودها الذَّكاء الاصطناعي-Artificial Intelligence ، وإنترنت الأشياء Internet Of Things، وسلاسل الكُتلة Block Chains ، والطابعات ثُلاثيَّة الأبعاد 3D Printers، والعُملات الافتراضية Virtual Currencies، والشَّرائح الذَّكيَّة المزروعة في جسم البشر Microchip Implant، وغيرها من التقنيات الذَّكيَّة. ومن شأن هذه الثَّورة أن تغير ليس فقط من هياكل الإنتاج وخصائص المُجتمعات وموازين القُوَّة، بل تغير أيضًا من المنظور المعرفي للبشر تجاه الأشياء بصورة عامة؛ فالبشرية أصبحت على وشك التَّحوُّل نحو جيل جديد من المُجتمعات، حيث يُنذر هذا التَّحوُّل بظهور مُجتمع فائق الذَّكاء تكون فيه اليد العُليا للآلة على الإنسان، وتتحقَّق فيه نبوءات أفلام الخيال العلمي بتآكل المُجتمع من داخله عبر إزالة الخطوط الفاصلة بين ما هو إنساني وما هو مادي، ويتعدى ما تمَّت تسميته مُجتمع المعلومات؛ ليظهر «مُجتمع ما بعد المعلومات».

هذا المُجتمع الخامس Fifth Society، الذي يمكن أن نطلق عليه في هذا الكتاب «مُجتمع ما بعد المعلومات»، يأتي بعد أربعة أجيال رئيسية مرَّت بها الإنسانية، وهي: مُجتمعات الصيد، والزراعة، والصناعة، والمعلومات، وأخيرًا المُجتمع الخامس أو «مُجتمع ما بعد المعلومات»، ذلك المُجتمع الذي تندمج فيه المعلومة والآلة مع عقل الإنسان، ويُعتبر الإنترنت أو الفضاء الإلكتروني أو النطاق الخامس Fifth Domain هو العمود الفقري لهذا المُجتمع، فبعد الأرض والبحر والجو والفضاء الخارجي، أصبح الفضاء الإلكتروني خامس الميادين التي تسعى البشرية لاستغلالها.

وعلى سبيل المثال، فبدلًا من أن يستخدم الفرد «خرائط جوجل» مثلًا للذهاب إلى مقصده كما هو الحال في مُجتمع المعلومات، ستقوم السيارة ذاتية

القيادة أو الطائرات المسيرة من دون طيار بذلك في مُجتمع ما بعد المعلومات، وبدلًا من إعطاء أوامر للرُّوبوتات للقيام ببعض الوظائف والمهام، فإنها سوف تقوم بصورة منفردة بتحليل المعلومات من المجسَّات وأجهزة الاستشعارات الموجودة في كل مكان، وتتخذ القرار بصورة ذاتية، وستقدم تقنيات إنترنت الأشياء خدمات للبشر تسبق احتياجاتهم وتوقعاتهم، وتصبح نظم الإدارة لا مركزيَّة بصورة كبيرة؛ بفضل تقنيات البلوك تشين.

ومع أن هذا التَّحوُّل ليس هو الأول الذي تُحدثه التطورات التكنولوجية عبر التاريخ، إلا أنه سوف يكون التَّحوُّل الأقوى؛ نظرًا لأنه سوف يغير من طرق التواصل بين الأفراد. ويتضح ذلك في تأثير الاختراعات التكنولوجية على طرق التواصل بينهم، بداية من اختراع آلة الطباعة الخشبية على يد الصينيين[1]، ثم اختراع التلغراف على يد «صمويل موريس»، مرورًا باختراع الهاتف على يد «جراهام بل»، ثم اختراع شبكة الويب على يد «تيم بيرنرزلي»[2]، ثم التطور الأبرز المتمثل في الشبكات الاجتماعية وتطبيقات الهواتف الذَّكيَّة وإنترنت الأشياء التي سهلت عملية التواصل بصورة كبيرة بين الأفراد.

وقد كان لظهور الفضاء الإلكتروني والشبكة العنكبوتية أثرٌ جوهريٌّ في الحياة البشرية، فسهولة استخدامها، ورخص تكلفتها، ساعدا على قيامها بأدوار مختلفة في الحياة البشرية، سواء تجارية، أو اقتصادية، أو معلوماتية، أو سياسية، أو عسكرية، أو أيديولوجية، أو غيرها من المهام التي يمكن أن تقوم بها، فالذي يُدير العالم حاليًا آحاد وأصفار في غاية الصغر. وقد أصبح جليًّا أن من يمتلك آليات توظيف هذه البيئة الإلكترونية الجديدة، يكون الأكثر قدرة على التأثير في سلوك الفاعلين المستخدمين لهذه البيئة.

1- Yu Tian, The Invention and Impact of Printing in Ancient China, Oct.28, 2007, Accessed 25 October 2016 on: https://bit.ly/1JCMwjH
2- Internet Hall Of Fame Innovator, Accessed on 25 October 2016, on: http://internethalloffame.org/inductees/tim-berners-lee

كما عمل الفضاء الإلكتروني على زيادة التفاعلات بين الأفراد عبر الدول، وسهولة تبادل المعلومات والبيانات، وعزَّز من التغيير الهيكلي لعملية صنع القرار داخل الدولة، من الاعتماد على المؤسسات الرسمية إلى تفاعل جهات وجماعات وأفراد رسمية وغير رسمية داخل الدولة عبر الشبكات الاجتماعية، والانتقال من مرحلة تبنِّي النموذج القائم على مركزية دور الدولة في صنع السياسات إلى مشاركة الأفراد في صياغة هذه السياسات، ومن الاعتماد على المؤسسات البيروقراطية في تقديم الخدمات إلى الاعتماد على شبكات الويب.

وقد أثَّرت التكنولوجيا أيضًا على الهويات والثقافات، وذلك بفعل تأثير العولمة التي أفرزتها هذه التطورات التكنولوجية، والتي جعلت العالم كله يبدو صغيرًا، فسهولة الاتصالات، ورخص تكلفتها سهَّلا عملية التواصل بين الحضارات والثقافات المختلفة، وأصبحت الثقافة الغربية المنتجة للتكنولوجيا هي الثقافة المهيمنة، حيث ساهمت التطورات التكنولوجية في تقديم الثقافة الغربية كثقافة عالمية للجميع؛ الأمر الذي يجعل الخصوصية الثقافية لبعض المُجتمعات موضع تهديد حقيقي.

أيضًا فقد غيَّرت التكنولوجيا من أشكال الحروب والصراعات البشرية على مدار العصور، فمن الحروب التقليدية التي استخدمت السيوف والرِّماح، ثم البنادق، والرشاشات، ثم القنابل النووية، والصواريخ العابرة للقارَّات، إلى نوع جديد من الحروب هو الحروب الإلكترونية التي تستخدم نوعًا آخرَ من الأسلحة المتمثلة في فيروسات الكمبيوتر التي لديها القدرة على إلحاق دمار يوازي دمار الأسلحة التقليدية، بل قد يفوقه في بعض الأحيان.

ولا يقتصر الأمر على ذلك، فالتكنولوجيا غيَّرت من أشكال الحكومات ووظائفها في بعض الأحيان، فمثلًا عرفت أدبيات العلوم السياسية الحكومة التقليدية التي تقدم خدماتها للجمهور عبر جهاز بيروقراطي مكتبي، ثم تطورت

إلى الحكومة الإلكترونية التي تعتمد على طرق الاتصال الحديثة، مثل الإنترنت في تقديم خدماتها للجمهور بسهولة ويُسر. ومع التطور التكنولوجي غير المسبوق بدأ عدد من الدول في تبنِّي نماذج الحكومات الذَّكيَّة القائمة على تقديم جميع خدماتها الحكومية إلى المواطن عبر الهاتف الذكي المتصل بالإنترنت.

وقد ألقت هذه التطورات التكنولوجية على الحكومات أعباءً عديدة، وذلك لأن التكنولوجيا سلاح ذو حدين، فكما يمكن استخدامها فيما يفيد البشرية، يمكن استخدامها أيضًا فيما يضرُّها؛ فإذا سبق المُجتمع الحكومات في استخدام التكنولوجيا الحديثة، مدفوعًا في ذلك بمبادرات شركات تكنولوجيا المعلومات؛ فإن ذلك قد يشكل تحدِّيًا للحكومات في كيفية إدارة العلاقات الجديدة الناشئة عن استخدام هذه التكنولوجيا، خاصة التهديدات الجديدة التي تطرحها، مثل الجرائم الإلكترونية على سبيل المثال، أو استخدام الطائرات التجارية من دون طيار، أو المخصصة للترفيه، في العمليات الإرهابية، أو استخدام الطابعات ثُلاثيَّة الأبعاد في صناعة الأسلحة.

ومن ثم، فإن التكنولوجيا قد غيَّرت بشكل كبير أنماط الحياة البشرية، سياسيًّا، وعسكريًّا، واقتصاديًّا، ومُجتمعيًّا، وغيَّرت من طرق التواصل بين الأفراد، وطوَّرت أجيالًا مختلفة من وسائل الحروب، وشكَّلت قوة دافعة للاقتصاد، وأظهرت أنماطًا مختلفة من السلوكيات، وخلقت أنواعًا جديدة من الثقافات، وغيَّرت من أشكال الحكومات وهياكل المدن والمُجتمعات، وضاعفت عدد التهديدات الجديدة التي لم تعتد عليها الدول في جميع مراحل حياة البشر السابقة.

وفي السياق ذاته، أفرزت التطورات التكنولوجية مفاهيم جديدة، مدفوعة باختراع الإنترنت، والهواتف الذَّكيَّة، وإنترنت الأشياء، ولا يزال بعضها غير واضحٍ، وبعضها الآخر لم يستقر بشكله النهائي كمفهوم مُكتمل الأبعاد، فمثلًا لا يزال هناك خلطٌ بين الإلكتروني Electronic، والسيبراني Cyber، والرقمي Digital، وعلى الرغم من هذا

الخلط، فإن هناك عددًا من المفاهيم التي استقرَّ استخدامها بصورة ما[1]، ومنها المفاهيم العسكرية، مثل القوة الإلكترونية Cyber Power، والصراع الإلكتروني Cyber Conflict، والردع الإلكتروني Cyber Deterrence، والحرب الإلكترونية Cyber War؛ ومنها المفاهيم السياسية، مثل الديمقراطية الرقمية Digital Democracy، والمواطنة الرقمية Digital Citizenship، والحكومة الإلكترونية EGovernment، والحكومة الذَّكيَّة Smart Government؛ ومنها المفاهيم الاجتماعية، مثل الجريمة الإلكترونية Cyber Crime، والتَّحرُّش الإلكتروني، والغش الإلكتروني، والمظاهرات الافتراضية؛ ومنها المفاهيم الاقتصادية، مثل التجارة الإلكترونية Ecommerce ، والعُملات الرقمية Digital Currencies، والأسواق الافتراضية Virtual Markets.

ولذا يمكن القول إن مسار هذا التغير الذي أحدثته التطورات التكنولوجيا في حالة حركة مستمرة وسريعة، وهو في طريقه إلى مزيد من التصاعد، مدفوعًا بمجموعة من مُحرِّكات القوى Driving Forces التكنولوجية، والتي يأتي على رأسها مواقع التواصل الاجتماعي، وتطبيقات الموبايل Mobile App، وتقنيات الواقع الافتراضي Virtual Reality، والطائرات من دون طيار «الدرونز»، والطابعات ثُلاثيَّة الأبعاد، وإنترنت الاشياء، والذَّكاء الاصطناعي، والحاسبات الكمومية Quantum Computers، والحوسبة السحابية Cloud Computing، والسيارات ذاتية القيادة Self-Drive Cars، والرُّوبوتات Robots، والعُملات الافتراضية؛ بصورة قد تدفع بقوة نحو إنشاء حياة جديدة تسيطر فيها التكنولوجيا على شكل الحياة البشرية، وتعيد صياغة جميع التفاعلات الشخصية، والمحلية، والدولية.

1- من الشائع في الأدبيات أن كلمة Cyber تشمل كل ما يتعلَّق بالإنترنت، وكلمة Digital تشمل كل ما يتعلَّق بنظم الحاسبات Computer Systems، وتشمل أيضًا عملية نقل وتحليل البيانات الرقمية التي تتكوَّن من آحاد وأصفار، أما كلمة Electronic فتشمل الأجهزة الإلكترونية نفسها، والحالة التي توجد عليها المعلومات بصورة غير مطبوعة.

ومن هنا جاءت فكرة إعداد هذا الكتاب، ليُلقي مزيدًا من الضوء على التطورات التكنولوجية التي من شأنها التأثير على حياة الأفراد في المستقبل القريب، بهدف فهم التهديدات والتحديات التي تطرحها من جانب، والمميزات والمكاسب التي تقدمها من جانب آخر؛ وذلك لتعظيم الاستفادة من مميزاتها وتفادي مخاطرها، وفي الوقت نفسه فهم التداعيات الناجمة عن تزايد الاعتماد على هذه التقنيات على المستوى القومي للدُّول، لأن من شأنها أن تغير من هيكل الوظائف وشكل الاقتصاد وتعيد صياغة عديد من المفاهيم المرتبطة بالقوة، والصراع، والحرب، بما يؤثر على جميع مظاهر الحياة الإنسانية.

ويضم الكتاب أربعة فصول، حيث يتناول الفصل الأول إرهاصات التَّحوُّل من مُجتمع المعلومات إلى «مُجتمع ما بعد المعلومات»، والخصائص الأولية لهذا المُجتمع الخامس؛ ثم يقدم الفصل الثاني التطورات التكنولوجيا والتقنيات الذَّكيَّة التي سوف تقود الثَّورة الصِّناعيَّة الرَّابعة بما تشمله من عملية تحديث سريع على جميع المستويات. واستتباعًا لذلك يناقش الفصل الثالث التهديدات الأمنية الجديدة للأمن الوطني للدُّول في «مُجتمع ما بعد المعلومات»، بينما يختتم الفصل الرَّابع والأخير ببحث تأثير هذه التقنيات الذَّكيَّة الجديدة على إعادة صياغة مفاهيم القوة والحرب والدفاع والردع في العلاقات الدولية.

الفصل الأول

المُجتمع الخامس.. التَّحوُّل نحو " مُجتمع ما بعد المعلومات "

بعد الثَّـورة الزراعيـة التـي حدثـت منـذ مـا يقـرب مـن عشـرة آلاف عـام؛ والثَّـورة الصِّناعيَّـة الأولى في القـرن الثامـن عشـر، والتـي قامـت علـى الفحـم، وقـوى البخـار؛ ثـم الثَّـورة الصِّناعيَّـة الثانيـة في القـرن التاسـع عشـر، والتـي قامـت علـى الكهرباء؛ فالثَّـورة الصِّناعيَّة الثالثـة التـي بـدأت فـي سـتينيات القـرن العشـرين، وقادهـا الكمبيوتـر، وعرفـت باسـم «الثَّـورة الرقميـة»؛ يؤكـد البروفيسـور «كلاوس شـواب» Klaus Schwab المؤسـس والرئيـس التنفيـذي للمنتـدى الاقتصـادي العالمي، في كتابه الثَّورة الصِّناعيَّة الرَّابعة The Forth Industrial Revolution، الصـادر في عـام 2016، أن العالـم علـى أعتـاب ثـورة صناعيـة رابعـة، يصفهـا بأنهـا «ثـورة لـم يشـهد التاريخ البشـري مثلهـا علـى الإطلاق، سواءً من حيث سرعتها، أو نطاقها، أو حتى تعقيداتها». ويقـود هـذه الثَّـورة عـدد مـن المُحـرِّكات الرئيسـية يحددهـا «شـواب» في: الـذَّكاء الصناعـي، والروبوتـات، والسـيارات ذاتيـة القيـادة، والطابعـات ثُلاثيَّـة الأبعـاد، والبيانـات العملاقـة، والعُمـلات الافتراضيـة، وإنترنـت الأشـياء، والنانوتكنولوجـي، والبيوتكنولوجـي، وتخزيـن الطاقـة، والحوسـبة الكموميـة.

> التغيير ليس فقط ضروري للحياة، بل هو الحياة
>
> **ألفين توفلر**

وقد ميَّز «ألفين توفلر» بين ثلاث موجات رئيسية أحدثت تغييرًا شاملًا في الحياة البشرية، وهي: الثَّورة الزراعية، ثم الثَّورة الصِّناعيَّة، ثم ثورة تكنولوجيا المعلومات التي أفرزت جميع المفاهيم المتعلقة بمُجتمع المعلومات. والآن بدأ العالم التَّحوُّل الأكبر نحو تبنِّي تقنيات الثَّورة الصِّناعيَّة الرَّابعة، بما يمهد الطريق لدخول مُجتمع جديد من البشرية؛ وهو ما يحاول هذا الفصل التعرض له عبر التمييز بين مُحرِّكات مُجتمع المعلومات ومُحرِّكات مُجتمع ما بعد المعلومات، ثم تحديد الخصائص الأولية لهذا المُجتمع الجديد، والذي تقوده مجموعة من المُحرِّكات التكنولوجية الجديدة والآخذة في الظهور.

أولًا: مقدمات التَّحوُّل من «مُجتمع المعلومات» إلى «مُجتمع ما بعد المعلومات»

تفرض الثَّورة الصِّناعيَّة الرَّابعة التي يشهدها العالم ضرورة مُلحَّة على الدول المتقدمة، خاصةً، كي تعيد النظر في استراتيجيتها التصنيعية من حيث إعادة بلورة أهداف تحافظ لهذه الدول على ريادتها خلال السنوات المقبلة؛ فالقوى المحركة للتنمية بمفهومها الشامل تتغير بسبب التطورات التكنولوجية المتسارعة، والتي تقودها التقنيات الذَّكيَّة، مثل إنترنت الأشياء، والذَّكاء الاصطناعي، والرُّوبوت، والطابعات ثُلاثيَّة الأبعاد، والحاسبات الكمومية، والهندسة الحيوية، وهو ما دفع الدول الصِّناعيَّة الكبرى في العالم إلى تبنِّي استراتيجيات جديدة تحافظ لها على تقدمها.

وعلى سبيل المثال، أصدر الرئيسي الأمريكي الأسبق «باراك أوباما»، في عام 2011 مبادرة «شراكة التصنيع المتقدم Advanced Manufacturing Partnership»[1] ، لتأمين القيادة الأمريكية في التصنيع المتقدم وتعزيز قدرتها التنافسية العالمية، خاصة في مجال التكنولوجيات الجديدة، وبعد ذلك، طرحت الإدارة شعار «إعادة تصنيع الولايات المتحدة وعودة وظائف التصنيع». وطرحت ألمانيا «استراتيجية التكنولوجيا العالية الجديدة The New High-Tech 2020 Strategy »[2] التي تركز على تحويل الأفكار المبتكرة في مجال التكنولوجيات الجديدة إلى تطبيقات واقعية. ووضعت بريطانيا «استراتيجية الصناعة والطاقة Energy and Industrial Strategy 2050»[3]، وطرحت اليابان «استراتيجية

1- President Obama Launches Advanced Manufacturing Partnership, National Institute of Standards and Technology, Created June 24, 2011, Updated November 27, 2017, accessed June 25, 2018, available on: https://bit.ly/2LdBe01

2- The new High-Tech Strategy, Federal Ministry of Education and Research (BMBF), accessed June 25, 2018, available on: https://bit.ly/2uBsxlE

3- Homes Of The Future, Now - Comfortable And Affordable To Heat, department for business, energy and industrial strategy, accessed June 25, 2018, available on http://www.buildingfor2050.co.uk

إنترنت الأشياء»[1]، والحفاظ على تقدمها على منافسيها في مجال الرُّوبوت. كما وضعت فرنسا في عام 2015 استراتيجية «صناعة المستقبل Industry Of The Future» التي تعد بمثابة خطة لإعادة التصنيع في فرنسا تشمل التركيز على التقنيات الذَّكيَّة، خاصةً في مجال المدن الذَّكيَّة، والنقل، والطب، والبيانات العملاقة[2]، وتبنَّت كوريا الجنوبية في عام 2016 «خطة النمو Growth Strategy»، التي تهدف إلى إعادة النظر في استراتيجيات التصنيع الكورية، والتركيز على مجالات الذَّكاء الاصطناعي، وإنترنت الأشياء، والسيارات الذَّكيَّة، والطب.

ولم تكن الصين غائبة عن هذا السباق الدولي الجديد نحو الابتكار والتصنيع المتقدم، ففي عام 2013، نظمت الأكاديمية الصينية للهندسة فريقًا ضم أكثر من مئة أكاديمي وعالم، لبحث اتجاه تطوير القطاع الصناعي الصيني، واستعراض إجراءات واستراتيجيات الدول الصِّناعيَّة المتقدمة، وقضايا القطاع الصناعي الصيني، وآثار التقدم التقني الرئيسية. وبعد عامين من الجهود، قدم الفريق بحثًا حول القطاع الصناعي الصيني، استندت إليه الحكومة الصينية في صياغة استراتيجية (صُنِعَ في الصين 2025)، التي أُعلِنَت في مايو [3]2015، وتهدف إلى دفع الارتقاء بالقطاع الصناعي الصيني وتحويله إلى قطاع متقدم، بما يساهم في تعزيز القدرة التنافسية الصِّناعيَّة الصينية، لتنضم الصين إلى صفوف دول العالم المتقدم في القطاع الصناعي، من حيث تخفيض استهلاك الموارد ورفع إنتاجية العمل وتعزيز القدرة على الابتكار التكنولوجي وتحسين الهيكل الصناعي والإسراع في تكامل المعلومات والتصنيع، وزيادة عدد براءات الاختراع والاستثمار في البحث والتطوير والعنصر البشري ونسبة الربح من المبيعات،

1- Leo Lewis, Internet of things tops Shinzo Abe's list of priorities, financial times, October 25, 2017, accessed June 26, 2018, available on: https://on.ft.com/2xoPBDw

2-Industry of the future, Le portail de l›Économie, des Finances, de l›Action et des Comptes publics, May 18, 2018, accessed June 26, 2018, available on https://www.economie.gouv.fr/files/files/PDF/pk_industry-of-future.pdf

3- تشو سن دي، صنع في الصين 2025 في الثورة الصناعية الرابعة، شبكة الصين، 24 يونيو 2018، تاريخ دخول 26 يونيو 2018، مُتاح على: http://arabic.china.org.cn/txt/2018-06/24/content_53244931.htm

على نحو يساعد في رفع مستوى القطاع الصناعي الصيني بشكل شامل ويجعل الصين في مقدمة الدول المنتجة لتكنولوجيات الثَّورة الصِّناعيَّة الرَّابعة.

إن هذه النماذج السابقة التي تؤكد سعي كبرى الدول الصِّناعيَّة إلى مواكبة الثَّورة الصِّناعيَّة الرَّابعة، تؤكد أن التَّحوُّل إلى مُجتمع «ما بعد المعلومات» قد بدأ يشق طريقه على أرض الواقع. وفي هذا السياق ظهر مصطلح (مُجتمع المعلومات) للمرَّة الأولى في اليابان في ستينيات القرن الماضي، وذلك في كتاب تحت عنوان «مقدمة لمُجتمع المعلومات «Introduction To An Information Society»، الصادر في عام 1968 للكاتبين «يونيجي ماسودا وكونيشي كوهوياما Yoneji Masuda And Konichi Kohyma»، وفي كتاب «مُجتمع المعلومات.. من المُجتمع الصلب إلى الناعم«The Information Society: From Hard To Soft Society»، الصادر في عام 1969 للكاتب «أوجيرو هياشي Ujiro Hayas-hi»؛ حيث ارتبط المفهوم في البداية بوصف التغيرات الاقتصادية والاجتماعية السريعة في المُجتمع، والناجمة عن عملية التحديث في المُجتمعات ما بعد الصِّناعيَّة [1](Post Industrial Societies).

وارتبط المفهوم منذ منتصف التسعينيات بصورة أكثر بالتطورات التكنولوجية داخل المُجتمع، والناتجة عن الموجة الثالثة المتمثلة في الثَّورة التكنولوجية. وعلى الرغم من استخدامه في البداية بقصد تحرير جميع أشكال الاتصالات، إلا أنه توسع تدريجيًّا ليشمل جميع الأبعاد المادية والبرمجية Hardware And Software الخاصة بالإنترنت، ثم توسع أيضًا ليشمل جميع الأدوات المتعلقة بالتعامل مع المعلومات، سواءً كانت جمعَ، أو تخزينَ، أو تداولَ، أو استرجاعَ، أو تحليلَ المعلومات[2].

1- László Z. Karvalics, Information Society – what is it exactly?(The meaning, history and conceptual framework of an expression), Budapest, March-May 2007. P 5-7, on: http://www.ittk.hu/netis/doc/ISCB_eng/02_ZKL_final.pdf
2-ibid.

ومع أنه يوجد عديد من التعريفات لمُجتمع المعلومات، لكن يُقصد به بصورة عامة أنه «ذلك المُجتمع الذي أصبحت فيه عملية إنشاء المعلومات وتوزيعها والتعامل معها هي السمة الرئيسية للأنشطة الاقتصادية والثقافية في هذا المُجتمع»[1].

وعلى سبيل المثال، يعرفه «دانيا بيل» بأنه «ذلك المُجتمع الذي يُشكل نفسه بصورة متماسكة حول المعرفة بهدف إدارة عملية الابتكار والتغيير داخل المُجتمع»، ويعرفه العالم الياباني «يونيجي ماسودا» بأنه «ذلك النمط من المُجتمعات الذي يصبح فيه امتلاك المعلومات، وليس الثروة المادية، هو القوى المحركة لعملية التَّحوُّل والتنمية بداخله، والذي تزدهر فيه أيضًا الابتكارات العقلية البشرية»[2].

ويُعد «فرانك ويبستر Frank Webster» من أبرز المُنظِّرين فيما يتعلق بنظريات مُجتمع المعلومات، وذلك في كتاب «نظريات مُجتمعات المعلومات Theories Of Information Societies ، الصادر في عام 1995، حيث يرى «ويبستر» أن هناك خمسة عناصر رئيسية تشكل مُجتمع المعلومات، تتمثل في أنه: (تكنولوجي Technological، واقتصادي Economic، ومهني Occupa-tional، ومكاني Spatial، وثقافي[3] Cultural.

وميز «ويبستر» بين مرحلتين رئيسيتين لتطورات تكنولوجيا المعلومات، وهما المرحلة الأولى، التي امتدت منذ نهاية السبعينيات وحتى بداية الثمانينيات، وفيها ظهرت الحاسبات الشخصية، وبدأ فيها إنشاء شبكات بين أجهزة الكمبيوتر وبعضها البعض، علاوة على الاعتماد على الأقمار الصِّناعيَّة في البث التلفزيوني.

1- Latif Al-Hakim, Global E-Government: Theory, Applications and Benchmarking: Theory, Applications, and benchmarking, Idea Group Publishing, 2007. P xi
2- László Z. Karvalics, Op cit. http://www.ittk.hu/netis/doc/ISCB_eng/02_ZKL_final.pdf
3 - Frank Webster, Theories of International society, International Library of Sociology, Third Edition, 2006, p 8-9

أما المرحلة الثانية، فقد بدأت منذ منتصف التسعينيات، وظهرت فيها أدوات التواصل والمعلومات، مثل البريد الإلكتروني، ورسائل الهاتف النصية، وتبادل المعلومات من خلال شبكة الإنترنت[1].

ويرى «ويبستر» أن الانشار السريع للإنترنت وتزايد الاعتماد عليه في مختلف المجالات، الاقتصادية والتعليمية والصِّناعيَّة، وحتى السياسية، قد دفع إلى القول إن النظام الجديد قد تم تطبيقه بالفعل، وهذا النظام يعتمد على تكنولوجيا الاتصالات بالأساس، وإن المستقبل سيوجد حيث توجد تكنولوجيا المعلومات، وإن الذي لا يلحق بعملية السبق هذه سوف يصبح أثرًا من الزمن، وإن تأثير التطورات التكنولوجية سوف يخلق مُجتمعات لا تتقيد بالأماكن Society Of Placeless Connectivity، ففي كل الأوقات وكل الأماكن، يكون المستخدم دائمًا متصلًا بالشبكة، بما لذلك من تداعياته إيجابية وسلبية[2].

ظهر مصطلح "مجتمع المعلومات" للمرة الأولى في اليابان في ستينيات القرن الماضي، وطرحه الكاتبان، يونيجي ماسودا وكونيشي كوهوياما، في عام 1968، لوصف التغيرات الاقتصادية والاجتماعية المتسارعة في المجتمع، والناجمة عن عملية التحديث في المجتمعات ما بعد الصناعية. وبحلول التسعينيات أصبح هذا المفهوم يشمل كافة الأبعاد المادية وغير المادية المتعلقة بالإنترنت، وذلك نتاجاً للتحولات الناتجة عن الموجة الثالثة من الثورة التكنولوجية.

وإذا كانت جميع هذه التطورات السابقة قد حدثت في عصر مُجتمع المعلومات، والذي نتج عن الجمع بين الثَّورة التكنولوجية والثَّورة الصِّناعيَّة الثالثة؛ فإن الثَّورة الصِّناعيَّة الرَّابعة التي بدأت أدراجها بالفعل تُعَدُّ ثورة لم يشهد التاريخ البشري مثلها على الإطلاق، لا في سرعة انتشارها، ولا في نطاقها،

1- Ibid. p9
2- Ibid. p10 -13

ولا في درجة تعقيدها، فالبشرية أمام ظاهرة تتحدى الزمان والمكان في قدرتها على الانتشار والتأثير في الدول والشعوب، وهي ظاهرة تجمع بين كل إنجازات الثورات السابقة عليها في الصناعة، والطاقة، والاتصالات، والمواصلات، وتضيف إليها إنجازات في مجالات جديدة تتداخل وتتكامل وتتبادل التأثير فيما بينها؛ ومن أبرزها: إنجازات في مجالات تكنولوجيا النانو، والتكنولوجيا الحيوية، وعلم الوراثة، والذَّكاء الاصطناعي، والرُّوبوتات، والطاقة... وكلها تنتج قواعد معلومات عملاقة وقدرات لا نهائية على تحليل البيانات والمعلومات، فضلًا عن وجود عُملات وأسواق افتراضية، ومخازن هائلة للطاقة، وسيارات ذاتية القيادة وطائرات من دون طيار، وطابعات ثُلاثيَّة الأبعاد، ومتاجر افتراضية ينتقي منها الناس الملابس والكتب، بل وقد تنتج روبوتات تصلح للزواج وتنتج أبناءً ولدوا من بويضات صناعية.

ويضع البروفيسور «كلاوس شواب» عدة أسباب لتبرير سبب اختلاف الثَّورة الصِّناعيَّة الرَّابعة عن سابقاتها، ولماذا تفوق تأثيراتها التأثيرات الناجمة عن الثورات الثلاثة السابقة، ومن هذه الأسباب ما يلي:

- **السرعة،** فعلى عكس الثورات الصِّناعيَّة السابقة، فإن هذه الثَّورة تسير بمتوالية هندسية تضاعفية، وليست بمتتابعة حسابية خطية. ومثال على ذلك هاتف آي فون الذي أعلنت عنه شركة أبل في عام 2007، والذي وجد منه في نهاية عام 2015 أكثر من ملياري جهاز ذكي حول العالم.

- **الاتساع والعمق،** فتأثير هذه الثَّورة الجديدة على جميع مجالات الحياة متسع وعميق، سواءً على المُجتمعات، أو الأفراد، أو الأعمال، أو الحكومات، فهي ثورة لن تغير فقط من آلية عمل الأشياء، بل تغير من الطريقة التي ننظر بها إلى أنفسنا أيضًا.

- التأثير على النظام، فمن شأن هذه الثَّورة أن تغير النظام القائم، سواءً بين أو داخل الدول والشركات والمُجتمع ككل.

وبالتالي، فإن العالم على أعتاب مرحلة جديدة من التاريخ البشري، حيث ينتقل من مرحلة مُجتمع المعلومات إلى مُجتمع ما بعد المعلومات، أو مُجتمع الذَّكاء الفائق، أو مُجتمع هيمنة الآلات، أو مُجتمع الذَّكاء الاصطناعي، أو مُجتمع السيبر Cyber، وجميعها مسميات تحاول وصف ما سيكون عليه شكل الحياة البشرية خلال السنوات القليلة المقبلة، وذلك على الرغم من صعوبة التنبؤ بما ستكون عليه، لكنها على الأقل تحدد المُحرِّكات التي تدفع نحو تشكيلها، والخصائص العامة التي تميزها، بما سوف تتركه من تداعيات مختلفة سوف تتطرق إليها السطور المقبلة.

ثانيًا: الخصائص الأساسية لـ«مُجتمع ما بعد المعلومات»

إن من شأن هذه التطورات التكنولوجية أن تعيد صياغة التفاعلات الإنسانية، سواء كانت اجتماعية، أو سياسية، أو اقتصادية، وأن تؤثر عليها بصورة مباشرة تدفع لبلورة مفهوم «مُجتمع ما بعد المعلومات»، والذي ستكون له خصائص مميزة ومختلفة عن مُجتمع المعلومات، من شأنها أن تؤثر على شكل الدولة ووظائف الحكومة، وتخلق أنماطًا جديدةً من التهديدات الأمنية التي تواجه الدول والأفراد، ويمكن أن تكرس التبعية الاجتماعية، فتنشأ تكنولوجيا للفقراء، وأخرى للأغنياء، وتعطي نفوذًا للآلات بصورة أكبر على الإنسان.

وكما سيأتي لاحقًا في الفصل الثاني حول المُحرِّكات الرئيسية والقوى الدافعة للثورة الصِّناعيَّة الرَّابعة، والتي سوف تشكل «مُجتمع ما بعد المعلومات»؛ فإن النظرة الأولى للتداعيات التي سوف تحدثها مثل هذه المُحرِّكات ستجعل المُجتمع الخامس ذا خصائص مختلفة ومميزة عن المُجتمعات السابقة عليه، **ومن أبرز ما يلفت النظر في هذا السياق ما يلي:**

1- فرص أكبر لتأثير الدول «سريعة التطور»، ولو كانت «صغيرة»

يُخبرنا الواقع بأن الثَّورة الصِّناعيَّة الرَّابعة تسير بالفعل وفق متوالية هندسية تضاعفية، وليس بمتتابعة حسابية خطية، فأعوام ثمانون تفصل بين اكتشاف «ألساندرو فولتا» لإمكانية توليد الكهرباء واستخدام اكتشافه، وأعوام ثمانية فقط تفصل بين إعلان شركة أبل عن الآي فون الأول لها في عام 2007 وانتشار أكثر من ملياري جهاز هاتف جوال ذكي حول العالم بحلول نهاية عام 2015.

وقد ارتبطت قدرة دولة ما على التأثير في العلاقات الدولية، وعلى تحقيق أهدافها الاستراتيجية، بما تمتلكه من موارد وفقًا لحجمها الجغرافي، وعدد سكانها، حيث اعتبرت عناصر مثل مساحة الدولة وعدد سكانها من أدوات

النفوذ في العلاقات الدولية، ولكن التطورات التكنولوجية الحالية قد تغير هذه النظرة التقليدية، فتعطي فرصة أكبر للدُّول صغيرة الحجم التي لديها قدرة على مواكبة التطور السريع في المجال التكنولوجي، على حساب الدول كبيرة الحجم التي تتأخر في مسايرة هذا التقدم.

وبالتالي، يمكن القول إن المستقبل يتشكل حاليًا من خلال الابتكارات التكنولوجية، التي يطغى عليها طابع السرعة، فالاستثمار في هذه التكنولوجية قد يزيد من قدرة الدول الصغيرة على التأثير في العلاقات الدولية التي ظلت لسنوات عديدة حكرًا على الدول الكبرى التي تعتمد بالأساس على مساحتها الجغرافية وعدد سكانها، بالإضافة إلى مواردها الطبيعية المحكومة بموقعها الجغرافي.

ولذلك، قد نجد في المستقبل القريب دولة صغيرة جدًّا مثل إستونيا بدأت في الاستثمار في تكنولوجيا المستقبل، ولديها عداء تاريخي مع دولة كبرى، مثل روسيا، تستطيع أن تلعب دورًا بارزًا في مواجهتها أكثر من ذي قبل.

2- تغيير شكل الحكومات وإعادة ترتيب أولوياتها:

تفرض التحديات التكنولوجية المقبلة على الحكومات أن تطور من أسلوبها، وتغير من أشكالها، فسرعة الإنترنت العملاقة، وحجم التخزين غير المسبوق مع صغر حجم أدوات التخزين، سيجعل المعلومات أكثر انتشارًا، وأصعب من حيث السيطرة عليها، وستصبح حركة الأفراد في السفر والانتقال أسرع وأسهل في الوقت نفسه، ولن تتمكن المُجتمعات المغلقة من وقف الأفكار المتدفقة إليها بأدواتها التقليدية، وستتوافر الأدوات الذَّكيَّة القابلة للارتداء والمتصلة بالإنترنت بصورة كبيرة بين الأفراد.

وهنا سوف يفرض العالم الافتراضي الكامل على الحكومات أن تكون أكثر ذكاءً في تقديم خدماتها للأفراد من خلال الحكومات الذَّكيَّة، وأكثر قدرة على حماية حدودها وأمن مُجتمعها من التهديدات التي تطرحها التطورات التكنولوجية، من خلال السبق في امتلاك وتطوير هذه الأدوات، حتى تكون قادرة على تنظيم استخدامها، وتلافي سلبياتها، وتقنين عملية تداولها، وأن تطور من أجهزتها الأمنية لكي تتعامل مع أنماط مختلفة من الجرائم، تكون فيها الأسلحة سهلة التصنيع من خلال أجهزة الكمبيوتر، وشديدة في التدمير من خلال وصولها لأكبر عدد من الأفراد.

3- تصاعد قدرة الفواعل من دون الدول على التأثير:

أتاحت التطورات التكنولوجية فرصة كبيرة للفواعل من دون الدول لزيادة قدرتها النسبية، حيث أصبح بإمكانها شراء المتفجرات عبر الإنترنت. ومع وجود الطابعات ثُلاثيَّة الأبعاد أصبحت قادرة على طباعة الأسلحة، وتحميلها على الطائرات من دون طيار، وتوجيهها عبر تطبيقات الهاتف الذكي، بصورة تهدد أمن الأفراد والمُجتمعات، وهو ما يخلق تحديات جمَّة أمام الدول لمراقبة حدوها الجغرافية، أو تحقيق الأمن المُجتمعي للأفراد، حيث تزداد قدرة الفواعل من دون الدول على المناورة بما تمتلكه من أدوات تكنولوجية قليلة الثمن كبيرة التأثير.

4- تصاعد الصراع بين الدول وشركات تكنولوجيا المعلومات:

لما كانت التكنولوجيا هي التي تقود تطور الحياة البشرية حاليًا، فإنه من المنطقي أن تكون أكبر أربع شركات عالمية من حيث القيمة السوقية في العالم خلال عام 2016 هي شركات تكنولوجيا المعلومات، وأولها شركة ألفابيت المالكة لجوجل، تليها أبل، ثم مايكروسوفت، ثم فيسبوك، مقارنة بشركة واحدة تكنولوجية هي مايكرسوفت في عام 2006، حيث تمتلك هذه الشركات وغيرها

المعلومات الكاملة عن جميع مستخدميها حول العالم، وقد يؤدي ذلك إلى صدام بين كثير من الدول وبعض هذه الشركات[1].

وبالفعل، فقد بدأت مثل هذه الأزمات كما ظهر في الصدام بين شركة جوجل والحكومة الصينية في عام 2010، والصدام المتكرر بين شركة أبل والحكومة الأمريكية، والصدام بين شركات مواقع التواصل الاجتماعي وبعض الدول، مثل إيران وتركيا، وذلك بسبب امتلاكها المعلومة التي يصعب على بعض الدول الحصول عليها.

ومع استمرار هذه الشركات في تطوير تكنولوجيات المستقبل مثل التخاطر، واللاي فاي Li-Fi، وأدوات التخزين، فإن احتمالات الصدام مع الدول قد تزداد مستقبلا، خاصة مع الدول النامية التي تعجز عن الاستثمار في هذه التكنولوجيا، ومن هنا قد تبدأ مرحلة جديدة من مراحل مشاركة الشركات الكبرى للدُّول في سيادتها المعلوماتية على مواطنيها.

تتداول الأدبيات عدة مُسمياتٍ مبدئية تحاول التعبير عن سمات مرحلة "مجتمع ما بعد المعلومات"، فهناك من يرى أنه "مجتمع الذكاء الفائق، ومن يقول إنه "مجتمع هيمنة الآلات، ومن يصفه بأنه "مجتمع الذكاء الاصطناعي والقوة السيبرانية". ولكن الثابت الوحيد في هذا كله أن الثورة الصناعية الرابعة سوف تُعيد تعريف ما هو اجتماعي وما هو سياسي وما هو اقتصادي، وما هو عالمي وما هو إنساني، وما هو قيمي وأخلاقي؛ لتظهر تحديات قيمية جديدة سوف يواجهها "مجتمع ما بعد المعلومات".

5- أنماط جديدة من الصراع على المعلومات الشخصية للأفراد:

في بداية انتشار الإنترنت في التسعينيات من القرن الماضي وبداية الألفينات، ظهرت بعض القوانين التي تحمي بيانات الأفراد عبر الإنترنت، وقد كانت بيانات الأفراد في هذه الفترة بيانات محدودة تقتصر على الاسم، والصورة، ورقم

1- ما أكبر 10 شركات في العالم من حيث القيمة السوقية؟، موقع الجريدة، 4 فبراير 2016، تاريخ الدخول 7 مارس 2016. https://bit.ly/2GBiIg0

التليفون، لكن مع التطورات التكنولوجية المستمرة وزيادة اعتماد الأفراد على التقنيات الذَّكيَّة؛ زاد معدل بيانات الأفراد الشخصية التي يمكن الحصول عليها عبر الإنترنت، حيث تمتد لتشمل بيانات الأفراد الحيوية مثل بصمة العين، والوجه، واليد، فضلًا عن البيانات الصحية والمرضية للمستخدم، بالإضافة إلى موقعه الجغرافي الحالي وأماكن تنقلاته في مختلف أرجاء المعمورة، وعديد من المعلومات الشخصية الأخرى، مثل نوعيَّة الأطعمة، والمشروبات، والملابس، والأفلام، والكتب، والموسيقي التي يفضلها المستخدم، ومواعيد عمله ونومه وغذائه، وتحديد شبكة أصدقائه وأفراد عائلته، بصورة تساعد في تكوين رسم تفصيلي عن حياة الفرد اليومية بفضل المعلومات الشخصية المتوافرة عن الفرد على الإنترنت.

وهنا فقد أضحت البيانات أساس العالم الرقمي الحالي، وجمعها ضروري للشركات بهدف تحسين الخدمات التي تقدمها لعملائها، سواء خدمات البحث عن المفضلات، أو خدمة الإعلانات، فضلًا عن استخدامها في تطبيقات الذَّكاء الاصطناعي وتعلم الآلات والسيارات ذاتية القيادة، وغيرها، مما يجعل المعلومات أحد أسباب الصراع في مُجتمع ما بعد المعلومات، فهي بمثابة الوقود المحرك لجميع التقنيات الذَّكيَّة.

6- فهم أدق لتوجهات المُجتمعات وأولويات الأفراد وتفضيلاتهم:

من خلال تحليل البيانات العملاقة يمكن، وبدقة كبيرة، تحديد اهتمامات الأفراد وأولوياتهم وتفضيلاتهم من خلال تحليل البيانات العملاقة الواردة من مختلف المنصات الرقمية كمواقع الإنترنت والأسواق الافتراضية ومواقع التواصل الاجتماعي، فضلًا عن البيانات الواردة من المجسَّات وأجهزة الاستشعارات وكاميرات المُراقبة المتوافرة في كل مكان في مُجتمع ما بعد المعلومات.

ويساهم هذا الأمر من ناحية في تحسين فهم المُجتمعات ومعرفة توجهات الأفراد بما يساعد في تطوير الخدمات وإرضاء الأذواق العامة، وصولًا إلى تحقيق السعادة البشرية؛ ولكنه يساهم من ناحية أخرى في تركز جميع المعلومات حول الأفراد لدى سلطة سياسية واحدة قد تسيئ استخدامها سياسيًّا من خلال ملاحقة المعارضين أو التأثير على توجهات الأفراد لاستمرار انتخاب فصيل سياسي دون غيره، وهو ما قد يؤدي إلى تهديد العملية الديمقراطية داخل الدولة نظرًا لتوافر المعلومات لجهة دون غيرها.

7- إعادة تعريف القيم الإنسانية وترسيخ مفهوم حقوق «الرُّوبوت»:

من شأن الثَّورة الصِّناعيَّة الرَّابعة أن تُعيد تعريف ما هو اجتماعي، وما هو سياسي، وما هو اقتصادي، وأن تعيد تعريف ما هو عالمي، وما هو إنساني، وما هو قيمي وأخلاقي؛ فتظهر التحديات القيمية التي يواجهها مُجتمع ما بعد المعلومات، ومنها قيمة «العدالة».. فماذا عن السيارة ذاتية القيادة إذا قتلت طفلًا أو امرأة، هل ستتم محاسبة السائق الآلي، أم صاحب السيارة، أم الشركة المنتجة لها، أم الدولة التي رصفت الطريق؟ أم أن هناك شخصًا آخرَ يتحمل المسؤولية؟!، وماذا عن قيمة العمل حينما يحل الإنسان الآلي محل البشر في خطوط الإنتاج؟، وماذا عن قيمة «الخصوصية» في ظل قيام الأفراد بأنفسهم بوضع معلوماتهم الخاصة على الشبكات الاجتماعية؟ وماذا عن قيم «الأسرة» التي تم اختزالها في جروب على الواتس آب؟ وماذا عن قيم «السيادة» في ظل حصول شركات تكنولوجيا المعلومات على جميع مواطني الدول؟ وماذا عن قيم الولاء والانتماء في سرعة تغير الأجهزة والأدوات الإلكترونية، وغيرها من الأسئلة التي تطرحها هذه الثَّورة الجديدة؟

إن الثَّورة الصِّناعيَّة الرَّابعة بحكم كونها منتجًا لتطور تكنولوجي ومعرفي وحضاري غربي تبدو بطبيعة الحال وكأنها تسكن بأريحية داخل منظومة قيمه

السائدة، حيث الرأسمالية الاستهلاكية المادية هي محفزة حركة الإنتاج والتوسع واستغلال الموارد وإنتاج الثروات، وحيث الفرد العاقل الرشيد الحر هو مركز هذا الكون ومصدر القيم والأخلاق... فهل تأتي الثَّورة الصِّناعيَّة الرَّابعة لتقود البشر إلى مزيد من تضخم وهم القدرة على إخضاع الطبيعة لذلك الإنسان الذي نصَّب نفسه إلهًا في هذا الكون لا يقيده دين أو عقيدة لتُعجِّل من وصول البشرية إلى فناء محتوم تدفعها نحوه دفعًا منظومة قيم وضعية؟ أم تأتي الثَّورة الصِّناعيَّة الرَّابعة لتصحح مسار بشرية أنهكتها الصراعات بين الأقوياء والأثرياء، وأرهقتها العصبية والعنصرية؛ وبالتالي فإن التكنولوجيا في مُجتمع ما بعد المعلومات تطرح تساؤلات أخلاقية وواقعية وسلوكية باتت تحتاج لإجابات تتناسب مع تداعيات الواقع الجديد.

ولا يقتصر الأمر على القيم الإنسانية، بل سيشمل الحديث أيضًا عن قيم الآلات الذَّكيَّة وحقوقها، لتظهر مجموعات حقوقية تطالب بحقوق الرُّوبوت في مُجتمع ما بعد المعلومات، فماذا إذا اعتدى الإنسان على الرُّوبوت، أو أعاقه عن القيام بوظيفته، أو أساء استخدامه، وماذا عن حقوق المواطنة والجنسية للرُّوبوتات، وهل يمكن وضع منظومة قانونية تحمي الرُّوبوت من الإنسان؟!

8- الأغنياء أكثر قُدرةً على الحصول على التقنيات فائقة الذَّكاء:

من شأن التطورات التكنولوجية المقبلة التي تختصر الزمان والمكان، مثل تحميل كميات عملاقة من البيانات عبر تكنولوجيا اللاي فاي، والصعود إلى الفضاء عبر مصاعد كهربائية، وتخزين مليارات الجيجابيت من خلال الحمض النووي، أن تكون للمُجتمعات الغنية القادرة على دفع تكلفة الحصول على هذه التكنولوجيا وتطويرها، فالذي يمتلك المال هو الذي يستطيع السفر من أقصى الكرة الأرضية إلى أقصاها في دقائق، أما من لا يمتلك المال الكافي فعليه أن يستعمل الطائرات التقليدية الحالية.

ومن ثم، فقد تقتصر التكنولوجيا الجديدة على الأغنياء، وتتحول بعض التكنولوجيات الحالية إلى الدول ذات الدخل المنخفض، فنحصل على تكنولوجيا للأغنياء، وأخرى للفقراء، ويستمر هذا الوضع إلى أن تنخفض تكلفة تصنيع المنتجات الجديدة وتصبح أسعارها في متناول الجميع.

9- خلق بيئات صناعية من الآلات الذَّكيَّة يصعب التحكم بها:

تعتمد التكنولوجيا الجديدة على تطوير الذَّكاء الاصطناعي، بحيث تصبح الآلات قادرة على اتخاذ قراراتها بصورة مستقلة أكثر من الوقت الحالي، وأن تنتشر هذه الآلات في الشوارع والطرقات، فنجد أن السيارات ذاتية القيادة تعرف طريقها ووجهتها، وقادرة على اتخاذ جميع قراراتها بصورة مستقلة، بداية من تحديد الطريق الأنسب الذي ستسلكه في مهمتها، مرورًا بتحديد سرعتها المناسبة وأماكن توقفها الملائمة، ونجد الطائرات من دون طيار يتم استخدامها في عديد من الأغراض، ليس فقط الأغراض العسكرية، بل المدنية والتجارية أيضًا، ويتزايد استخدام التَّطبيقات الذَّكيَّة القادرة على أن تحمي نفسها من الهجمات السيبرانية والفيروسات، وأن نجد هواتف تشحن ذاتيًّا... وجميع هذه التطورات وغيرها، من شأنها أن تخلق بيئة جديدة ركيزتها الأساسية هي الذَّكاء الاصطناعي، وتستطيع فيها الآلات أن تتخذ قرارها بصورة مستقلة نوعًا ما عن الإنسان، فتكون المحصلة النهائية هي بيئة يصعب على الإنسان التحكم بها.

يعتقد بعض المنظرين أن العلاقة بين الآلة والإنسان في "مجتمع ما بعد المعلومات" سوف تترك بعض التداعيات الإنسانية السلبية، لأن من شأن ذلك أن يفصل الإنسان تدريجيًا عن محيطه الاجتماعي البشري الطبيعي، وأن يُفقد العلاقات البشرية مرونتها التقليدية، ويجعلها أكثر صلابة وجمودًا، فتتحول طرق التفكير والتفاعلات البشرية من التعقيد المفيد إلى التنميط ولو كان منتجًا.

10- تغيير هيكل وشكل الوظائف، واختفاء بعض المهن:

من المتوقع أن يؤثر انتشار تطبيقات الذَّكاء الاصطناعي على شكل الوظائف وتفاصيلها، فالمُقابلات الخاصة بالتوظيف من الممكن أن تتم قريبًا مع أجهزة كمبيوتر قادرة على تحليل أدق التفاصيل والوصول إلى تعابير الوجه.

ليس هذا فحسب، بل إن التكنولوجيات الجديدة قد تخلق الوظائف، وهو ما أثبته التاريخ، حيث إنه دائما وأبدًا ما كانت تعزز الابتكارات التكنولوجية إنتاجية العمال وتخلق منتجات وأسواقًا جديدة، مما أتاح فرص عمل جديدة في الاقتصاد، وهو الأمر الذي لن يكون مختلفًا بالنسبة لتطبيقات الذَّكاء الاصطناعي، مثل: الطباعة ثُلاثيَّة الأبعاد، والرُّوبوتات، وهو ما أقرَّته إدارة الشؤون الاقتصادية والاجتماعية التابعة للأمم المتحدة UN DESA في تقريرها الصادر عام 2017، والتي أكدت أن تطبيقات الذَّكاء الاصطناعي ستعمل بدورها على خلق فُرص عمل، خاصة إذا كان هذا مُصاحبًا لوجود مجموعة من الضوابط المتمثلة في القواعد القانونية والتنظيمية والاجتماعية – السياسية التي تمنع بدورها عديدًا من الوظائف من الاختفاء، وخير دليل على ذلك أنه في عام 2016 تم القضاء على واحدة فقط من أصل 270 مهنة مُدرجة في تعداد الولايات المتحدة لعام 1950 بسبب الأتمتة، أو تحويلها إلى الاعتماد على التكنولوجيا[1].

ولعل توسع استخدام الذَّكاء الاصطناعي والتقنيات الذَّكيَّة في عديد من القطاعات الاقتصادية والاجتماعية والسياسية يُقابله تقليص في العمالة البشرية والاعتماد على الذَّكاء البشري، حيث أصبحت أجهزة الحاسب الآلي تتعدى بشكل متزايد على المجالات التي كانت تعتبر من قبل بشرية بشكل حصري.

1-Department of Economicand Social Affairs, United Nations, Will robots and AI cause mass unemployment? Not necessarily, but they do bring other threats, New York, 13 sep., 2017, Available at: https://bit.ly/2xjFLmo

وقد مكَّن التقدم المذهل في مجالات الذَّكاء الاصطناعي المختلفة، مثل: الرُّوبوتات، والطباعة ثُلاثيَّة الأبعاد، وعلم الوراثة، وأجهزة الكمبيوتر من أداء مهام المهندسين المعماريين، والأطباء، والمؤلفين الموسيقيين، وحتى أساتذة الرسم.

وفي هذا الصدد عبَّر الخبراء الاقتصاديون عن قلقهم بشأن ذلك الأمر، حيث إن الاعتماد المُتنامي على الذَّكاء الاصطناعي من شأنه أن يؤدي إلى خسارة كثير من الوظائف، فقد أظهرت آخر بيانات إدارة الشؤون الاقتصادية والاجتماعية التابعة للأمم المتحدة UN DESA أنه «بحلول عام 2050 من المتوقع أن يصل عدد السكان إلى 9.8 مليار شخص، وأكثر من 6 مليارات منهم سيكونون في سن العمل، وفي هذه الأثناء سيكون هناك سعي لإيجاد فرص عمل لنحو 71 مليون شاب حول العالم»؛ ومن ثم يُعد هذا من أسباب اعتبار التكنولوجيات الجديدة تهديدًا كبيرًا لأسواق العمل[1].

وفي دراسة نُشرت في هذا الصدد، وتم عرضها في منتدى دافوس الاقتصادي في عام 2018، أشارت إلى أن 1.4 مليون وظيفة في الولايات المتحدة فقط مُهددة بسبب التقنيات الجديدة بحلول عام 2026، وأن 47% من الوظائف مُهددة بأن تتحول إلى وظائف تعتمد على الحاسب الآلي[2].

1- Department of Economicand Social Affairs, United Nations, Op. Cit.
2- Aaron Smith, Public Predictions for the Future of Workforce Automation, PEW Research Center, 2016, p: 2

الفصل الثاني

مُحرِّكات ثورية.. القوى الدَّافعة لـ "مُجتمع ما بعد المعلومات"

هناك عدد من القوى المحركة التي تساهم بقوة في التَّحوُّل نحو «مُجتمع ما بعد المعلومات»، والتي تمثل أهم عناصر الثَّورة الصِّناعيَّة الرَّابعة، وأبرزها تقنيات الذَّكاء الاصطناعي، والطابعات ثُلاثيَّة ورباعية الأبعاد، وسلسلة الكُتلة، وإنترنت الأشياء، والعُملات الافتراضية، والبيانات العملاقة، بالإضافة إلى عدد آخر من التقنيات، مثل خدمات الحوسبة السحابية، وتطبيقات الهواتف الذَّكيَّة، ونظم إدارة احتياجات العملاء، والشَّرائح الإلكترونية الذَّكيَّة التي يتم زرعها في الأجساد البشرية، فضلًا عن عدد كبير آخر من التطورات التقنية ذات التأثير الملموس أيضًا، ولكنه ليس بحجم هذه التقنيات.

> الذكاء الاصطناعي أسوأ ما حدث للبشرية
>
> ستيفن هوكينج

وتمثل هذه المُحرِّكات بداية تدشين المُجتمع الخامس للبشرية، لكنها بالطبع ستخضع لعمليات التطوير والتحديث السريع داخل «مُجتمع ما بعد المعلومات»، فتتغير خصائصها كي تكون أقل تكلفة، وأكثر كفاءة، وأسهل في الاستخدام، ويمكن الحصول عليها في أي مكان، هذا بالإضافة إلى ظهور تقنيات أخرى متقدمة يصعب التنبؤ بها مستقبلًا نتيجة إدخال الحسابات الكمومية والأقمار الصِّناعيَّة فائقة الصغر، لتنشأ تقنيات أكثر تقدمًا ترسخ هذا المُجتمع الجديد.

أولًا: الذَّكاء الاصطناعي

قام «جون مكارثي» John McCarthy سبتمبر 1927 – 23 أكتوبر 2011)، الملقب بأبي الذَّكاء الاصطناعي، بصك هذا المصطلح في عام 1956. ووفقًا له، فإن الذَّكاء الاصطناعي هو «علم هندسة إنشاء آلات ذكية، وبصورة خاصة برامج الكمبيوتر»[1]، أي إنه علم إنشاء أجهزة وبرامج كمبيوتر قادرة على التفكير بنفس الطريقة التي يعمل بها الدماغ البشري، تتعلم مثلما نتعلم، وتقرر كما نقرر، وتتصرف كما نتصرف.

وبهذا المعنى، فإن الذَّكاء الاصطناعي هو عملية مُحاكاة الذَّكاء البشري عبر أنظمة الكمبيوتر، فهي محاولة لتقليد سلوك البشر ونمط تفكيرهم وطريقة اتخاذ قراراتهم، والتي تتم من خلال دراسة سلوك البشر عبر إجراء تجارب على تصرفاتهم ووضعهم في مواقف معينة ومُراقبة رد فعلهم ونمط تفكيرهم وتعاملهم مع هذه المواقف، ومن ثم محاولة مُحاكاة طريقة التفكير البشرية عبر أنظمة كمبيوتر معقدة.

ولمَّا كان الذَّكاء الاصطناعي هو أنظمة كمبيوتر تحاكي البشر في تصرفاتهم، فإن هذا لا يعني أن أي قطعة برمجية تعمل من خلال خوارزمية معينة، وتقوم بمهام محددة تعتبر ذكاءً اصطناعيًّا، فلكي نطلق هذا المصطلح على نظام كمبيوتر لا بد أن يكون قادرًا على التعلم وجمع البيانات وتحليلها واتخاذ قرارات بناءً على عملية التحليل هذه، بصورة تحاكي طريقة تفكير البشر، وهو ما يعني توافر ثلاث صفات رئيسية هي[2]:

1-Artificial Intelligence, Toutorials point, 2015, accessible at: https://www.tutorialspoint.com/artificial_intelligence/artificial_intelligence_tutorial.pdf
2- AI (Artificial Intelligence), Techtarget, accessible at: https://bit.ly/2AhNLHU

1- القدرة على التعلم، أي اكتساب المعلومات ووضع قواعد استخدام هذه المعلومات.

2- إمكانية جمع وتحليل هذه البيانات والمعلومات وخلق علاقات بينها، ويساعد في ذلك الانتشار المتزايد للبيانات العملاقة Big Data.

3- اتخاذ قرارات بناءً على عملية تحليل المعلومات، وليس فقط مجرد خوارزمية تحقق هدفًا معينًا.

وفي ضوء ما سبق، فإن خوارزمية البحث على «جوجل» مثلًا لا تصبح ذكاءً اصطناعيًّا، إلا إذا توافرت فيها هذه الصفات الثلاث، فإذا قام أحد الأفراد بالبحث مثلًا عن السياحة في أبوظبي، وأدركت خوارزمية البحث هذا المطلب وأجابته عليه في حدود البحث عن السياحة في أبوظبي فقط، فإن ذلك لا يعد ذكاءً اصطناعيًّا، ولكي يكون كذلك، لا بد أن تجمع الخوارزمية بيانات أكثر، وتعرض مقترحات إضافية، أي أن يقوم النظام من تلقاء نفسه بترشيح إعلانات لهذا الشخص عن عروض السياحة في أبوظبي، وأفضل خطوط الطيران التي يمكن أن يسافر من خلالها، وأي الفنادق التي يمكن أن يسكن فيها أثناء رحلته، ثم يبدأ بترشيح بعض الأماكن والمعالم السياحية التي يمكن زيارتها في أبوظبي، وبهذا يقدم النظام أكثر من مجرد عملية بحث عادية، وهو ما يحدث بالفعل عبر «جوجل».

تثير مخرجات الذكاء الاصطناعي حتى الآن آراءً متناقضة تمامًا بشأن تداعيتها المتوقعة، فهناك فريق يعتقد أنه سوف يسهل ويحسن حياة البشرية بشكلٍ غير متناهٍ، وهناك من يرى أنه سوف يخلق تداعياتٍ سلبية وخيمة تفوق إيجابياته، ومن هذا الفريق عالم الفيزياء الشهير "ستيفن هوكينج" الذي أشار إلى أن المزيد من تطوير الذكاء الاصطناعي قد يمهد لنهاية الجنس البشري.

1- أنواع الذَّكاء الاصطناعي:

بصورة عامة، يمكن تقسيم أنواع الذَّكاء الاصطناعي إلى ثلاثة أنواع رئيسية، تتراوح من رد الفعل البسيط إلى الإدراك والتفاعل الذاتي، وذلك على النحو التالي[1]:

أ- الذَّكاء الاصطناعي الضيق أو الضعيف Narrow AI or Weak AI:

هو أبسط أشكال الذَّكاء الاصطناعي، حيث تتم برمجة الذَّكاء الاصطناعي للقيام بوظائف معينة داخل بيئة محددة، ويُعتبر تصرفه بمثابة رد فعل على موقف معين، ولا يمكن له العمل إلا في الظروف البيئية الخاصة به. ومن الأمثلة على ذلك الرُّوبوت «ديب بلو»، الذي صنعته شركة آي. بي إم. IBM، والذي هزم «جاري كاسباروف» بطل الشطرنج العالمي.

ب- الذَّكاء الاصطناعي القوي أو العام General AI or Strong AI:

يتميز هذا النوع بالقدرة على جمع المعلومات وتحليلها وعمل تراكم خبرات من المواقف التي يكتسبها، والتي تؤهله لأن يتخذ قرارات مستقلة وذاتية. ومن الأمثلة على ذلك السيارات ذاتية القيادة، وروبوتات الدردشة الفورية، وبرامج المساعدة الذاتية الشخصية.

ج - الذَّكاء الاصطناعي الخارق Super AI:

هو عبارة عن نماذج جديدة لا تزال تحت التجربة وتسعى لمُحاكاة الإنسان. ويمكن هنا التمييز بين نمطين أساسيين له، الأول: يحاول فهم الأفكار البشرية، والانفعالات التي تؤثر على سلوك البشر، ويملك قدرة محدودة على التفاعل الاجتماعي. أما الثاني: فهو نموذج لنظرية العقل، حيث تستطيع هذه النماذج

1- أنواع الذكاء الاصطناعي، مرصد المستقبل، مؤسسة دبي للمستقبل، متاح على الرابط التالي: https://goo.gl/Yo9Dp3 (تاريخ المطالعة: 28 يناير 2016).

التعبير عن حالتها الداخلية، وأن تتنبأ بمشاعر الآخرين ومواقفهم وتتفاعل معها، أي إنها هي الجيل القادم من الآلات فائقة الذَّكاء.

2- أبرز تطبيقات الذَّكاء الاصطناعي:

أظهر الذَّكاء الاصطناعي تقدمًا تقنيًّا كبيرًا على مدى السنوات الماضية في عديد من المجالات الحياتية، وهو ما نتج عنه عديد من الإيجابيات، مثل التطور الصحي، وزيادة الأمن البيئي والبشري، وخلق فرص عمل مختلفة، وغيرها.

ولكن على الجانب الآخر، أثار انتشار تطبيقات الذَّكاء الاصطناعي تخوف كثيرين، خاصة مع توقعاتهم حول تأثير تطبيقات الذَّكاء الاصطناعي على زيادة معدلات البطالة، وعدم دقة البيانات، التي قد ينتج عنها تحيز في اتخاذ القرارات وغيرها من المخاوف.

ومع الأخذ في الاعتبار وجهات النظر المختلفة لانتشار تطبيقات الذَّكاء الاصطناعي، إلا أنه يجب الاعتراف بوجود تحديات تواجه عملية الانتشار، أهمها التكلفة المادية، والتعاون بين المؤسسات للحصول على البيانات الضخمة اللازمة، وغيرها، لكن هذه التحديات لن تعوق التوسع في استخدام تقنيات الذَّكاء الاصطناعي في شتَّى المجالات؛ فمنذ عام 2000 تضاعف عدد الشركات الناشئة Start Up العاملة في مجال الذَّكاء الاصطناعي نحو 14 ضعفًا، وتضاعف الاستثمار في هذا المجال 6 مرَّات، وتزايد عدد الوظائف التي تتطلب مهارات ذكاء اصطناعي منذ عام 2013 نحو أربع مرَّات ونصف المرَّة[1]، وهو ما جاء أسرع كثيرًا مما كان متوقعًا عن ذي قبل، ولذا يرى الخبراء والمتخصصون أن ذلك التقدم سيستمر بوتيرة أسرع في جميع مجالات الحياة تقريبًا.

1- Louis Columbus, 10 Charts That Will Change Your Perspective On Artificial Intelligence›s Growth, FORBES, Jan 12, 2018, on: https://bit.ly/2SujsoO

وتتضح مظاهر الذَّكاء الاصطناعي في المدن الذَّكيَّة، في عدة تقنيات، منها الرُّوبوتكس Robotics، وهو ذلك الفرع من التكنولوجيا المتعلق بعملية تصميم وبناء وتشغيل تطبيقات مختلفة من الرُّوبوتات أو الإنسان الآلي، والذي يُعد واحدًا من أكثر تطبيقات الذَّكاء الاصطناعي تقدمًا، حيث يهتم ببناء هيكل مادي يعمل وفق منطق بشري، ويمكن برمجته أو توصيله بالحاسب الآلي ليؤدي مهامَّ معينة، ولكونها آلة ذكية فسوف يُترَك لها قدر من حرية التصرف وفق ما تواجهه من مواقف. وقد وجهت كثير من الشركات خلال السنوات القليلة الماضية جهودها نحو بناء نظام آلي قادر على قيادة السيارات، مثل شركتي «جوجل» و«تسلا»، ومؤخرًا «أبل»، وغيرها من الشركات، بصورة سوف تحل السائق الآلي محل السائق البشري[1].

كما تقوم المدن الذَّكيَّة أيضًا على نظم المُراقبة الشاملة Mass Surveil-lance باستخدام تقنيات الذَّكاء الاصطناعي، بهدف تحقيق الأمن فيها، ومُراقبة الخطر واكتشاف مصادر التهديد، وبصورة خاصة في الأماكن العامة، والتي يمكنها أن تميز حركة الأفراد، وتتوقع الحركات التي قد تشكل تهديدًا وتطلق إنذارًا بها، بل يمكن لها أيضًا أن تميز الوجوه وتتعرف على هوية الأشخاص الموجودين بالمكان[2].

ويشهد عديد من دول العالم استخدامًا متصاعدًا للرُّوبوتات التي يتم توجيهها عن بُعد، والتي تعد إحدى المراحل الأساسية المهمة في اتجاه تطوير «الأسلحة ذاتية التشغيل»، والمستقلة تمامًا، حيث تمتلك الولايات المتحدة مثلًا نحو 20 ألف وحدة من الأسلحة القاتلة ذاتية التشغيل، وتقوم هذه الأسلحة بعدة أدوار، تتمثل في جهود الرقابة والرصد المستمرة، وإطلاق النيران، وحماية

1- ARTIFICIAL INTELLIGENCE AND LIFE IN 2030, Stanford, Accessed Jan 30, 2017, on: https://stanford.io/2bRx6C2
210Examples of Artificial Intelligence You're Using in Daily Life, Beebom, September 16, 2016, on http://beebom.com/examples-of-artificial-intelligence/

القوات، بالإضافة إلى مواجهة العبوات الناسفة، وتأمين الطرق، والإسناد الجوي عن قُرب.

وتُعَدُّ الطائرات من دون طيار المُسيَّرة أيضًا أحد نماذج الرُّوبوتكس، حيث انتشر هذا الشكل من الطائرات في كثير من الأعمال، منها ما هو مُسيَّر من خلال غرفة تحكم بشرية، ومنها ما هو قادر على اتخاذ قراراته بنفسه، مثل تتبع حركة غير منطقية، كما في الطائرات التي تُستخدم في مُراقبة الحدود والمحاصيل الزراعية، أو الطائرات القادرة على توصيل الطرود والأطعمة، أو تلك الطائرات المستخدمة في التصوير الفوتوغرافي والسينمائي، وغيرها من عشرات الاستخدامات المدنية[1].

ومن نماذج الذَّكاء الاصطناعي أيضًا برامج المساعدة الذاتية الصوتية Sound Assistance Programs، وهي تلك البرامج التي تتلقى الأوامر الصوتية من المستخدم للقيام بوظائف معينة، أو تتفاعل مع المستخدم عبر تقنية الصوت، حيث اتجهت كبرى الشركات في العالم إلى إنشاء نماذج من هذه البرامج؛ فأنشأت شركة أبل SIRI، وشركة أمازون Alexa، وشركة مايكروسوفت Cor-tana، وشركة جوجل Google Assistant، وشركة فيسبوك Javris، وأنشأت شركة نوكيا Viki[2]، إذ تساعد هذه التقنيات في تسهيل عملية التواصل بين الإنسان الآلة بشكل كبير وأسهل.

3- التهديدات التي يطرحها الذَّكاء الاصطناعي:

تنقسم آراء الخبراء حول الذَّكاء الاصطناعي إلى فريقين رئيسيين، الأول يرى

1- ARTIFICIAL INTELLIGENCE AND LIFE IN 2030, Stanford, Accessed Jan 30, 2017, on: https://ai100.stanford.edu/sites/default/files/ai_100_report_0901fnlc_single.pdf

2- Jeff Dunn, we put Siri, Alexa, Google Assistant, and Cortana through a marathon of tests to see who›s winning the virtual assistant race -here›s what we found, Businessinsider, Nov. 4, 2016, on https://read.bi/2mjwZmT

أن الذَّكاء الاصطناعي يحسّن حياة الأفراد ويجعلها أكثر سهولة، كما صرح به «مارك زوكربرج»، رئيس ومؤسس موقع فيسبوك، وأن كل من يخشى الذَّكاء الاصطناعي فهو «يأسف على الوهم ويغالط البشر»، كما أشار الملياردير الأمريكي «مارك أندرسون».

أما أنصار الفريق الآخر فيرون أن الذَّكاء الاصطناعي ستكون له تداعيات سلبية وخيمة على البشرية، وسيؤدي في نهاية المطاف إلى حرب عالمية مقبلة، بحسب تصريحات «أيلون موسك»، رئيس ومؤسس شركتي تسلا، وسباس إكس، بل يذهب عالم الفيزياء العملاق «ستيفن هوكينج» إلى أبعد من ذلك، إذ يشير إلى أن تطوير ذكاء اصطناعي كامل قد يمهد لنهاية الجنس البشري». وبهذه الصورة السابقة يكون الذَّكاء الاصطناعي قد انحصر في ثنائية إما سعادة البشرية أو تدميرها.

لكن، على الرغم من إدراك كل فريق أن الفريق الآخر يجانبه الصواب في بعض الأمور، فإن تحيز كل منهما لرأيه يعكس حالة القلق التي تنتاب الجميع تجاه الذَّكاء الاصطناعي، وهذا القلق لم يتوقف عند الخبراء والعلماء فقط، بل صرح الرئيس الروسي «فلاديمير بوتين»، بأن «من سيقود الذَّكاء الاصطناعي سيحكم العالم»، لافتًا الانتباه إلى أهميته ومخاطره في التوقيت نفسه.

إذن، فالذَّكاء الاصطناعي ثورة تكنولوجية لها مميزاتها كما أن لها تهديداتها، بالضبط كاختراع الطائرات التي يمكن أن تجعل حياة البشر أسهل وأسرع، أو أن تقضي عليهم عبر استخدامها في القتل والتدمير، فالثَّورة التي سيحدثها الذَّكاء الاصطناعي هي ثورة شاملة على مختلف المستويات، الأمنية، والاقتصادية، والاجتماعية، وهو ما دفع دولة الإمارات العربية المتحدة، على سبيل المثال، إلى إنشاء وزارة للذكاء الاصطناعي؛ للاستفادة من هذه الثَّورة المقبلة، وتلافي مخاطرها المستقبلية.

ومما لا شك فيه، فإن هناك عديدًا من التداعيات المترتبة على زيادة الاعتماد على تقنيات الذَّكاء الاصطناعي، سواء كانت أمنية، أو اجتماعية، أو اقتصادية، أو حتى إنسانية، وقانونية. فمن الناحية الاقتصادية، سوف يؤثر الذَّكاء الاصطناعي على حجم ونوعية الوظائف وفرص العمل المتاحة، حيث من المتوقع أن يؤثر الرُّوبوت تأثيرًا سلبيًّا على الوظائف في مجال الصناعات التحويلية وصناعة السيارات والأدوات الكهربائية، بالإضافة إلى خدمة العملاء، بينما يؤثر إيجابيًّا على وظائف أخرى، مثل الهندسة الميكانيكية، وهندسة الأمن والسلامة، وصناعة البرمجيات والإلكترونيات، وهذا الأمر ينطبق أيضًا على السيارات ذاتية القيادة والطائرات من دون طيار، والطابعات ثُلاثيَّة الأبعاد، حيث تهدد وظائف وتنعش وظائف أخرى.

يكاد يجمع المحللون والمتخصصون على أن التداعيات المُحتملة للذكاء الاصطناعي، اجتماعياً وإنسانياً واقتصادياً، تستلزم منذ الآن البحث عن آليات تنظيمية وأخلاقية تحفظ حقوق البشر، سواءً لجانب حماية الوظائف المهددة بالاختفاء، أو لجانب طغيان الأبعاد المادية بشكل كامل على الأبعاد المعنوية في سلوكيات الناس، أو لجانب وضع منظومة قيمية تحكم العلاقة بين الإنسان والآلة في عصر قد تتفوق فيه الآلة على الإنسان.

أما من المنظور الأمني، فإن أحد التداعيات الخطيرة التي تطرحها تقنيات الذَّكاء الاصطناعي هي تهديدها لحق البشر في الحياة، ويتضح ذلك في حالة الأنظمة القتالية المستقلة، مثل الطائرات من دون طيار التي تحمل أسلحة، أو الرُّوبوتس الموجودة في أرض المعارك للقيام بوظائف محددة، حيث تكمن الخطورة هنا في أن هذه الأجهزة مصممة من أجل التدمير أساسًا.. فماذا يحدث إذا وقعت في يد الشخص الخطأ، أو تم اختراقها لقصور أو خطأ بشري في إجراءات التأمين والتلاعب بالخوارزميات التي تتحكم فيها، فهنا سوف تكون النتائج كارثية.

ويضيف البعض الآخر بعض التداعيات الإنسانية والأخلاقية، فزيادة الاحتكاك مع الآلات، من شأنه أن يفصل الإنسان تدريجيًّا عن محيطه الطبيعي الاجتماعي البشري، وأن يُفقد العلاقات البشرية مرونتها التقليدية، ويجعلها أكثر صلابة وجمود، فتتحول طرق التفكير والتفاعلات البشرية من التعقيد المفيد، إلى التنميط ولو كان منتجًا، ويصبح الهدف من العلاقات الإنسانية ماديًّا بعد أن كان معنويًّا بالأساس.

وفي ضوء ما سبق، يصبح التساؤل الرئيسي: ما القواعد الأخلاقية التي تحكم العلاقات بين الإنسان والآلة، وبين الآلة والآلة أيضًا؟ وما المنظومة القيمية أو مجموعة القواعد العُليا التي يجب أن تعمل في إطارها هذه العلاقات «البشرية – الرُّوبوتية»؟، كما يثار التساؤل حول الكيفية التي سيتم من خلالها التعامل مع التجاوزات التي تصدر عن الآلات، مثل اعتداء الآلة على الإنسان، كأن تقتل السيارة ذاتية القيادة إنسانًا، أو أن يتم توظيف كاميرات المُراقبة في انتهاك خصوصية الأفراد، أو أن يتسبب تعليم الآلات في ضمور القدرات البشرية، أو أن تتحكم خوارزميات البحث على الإنترنت في أنماط تفكيرنا وأولوياتنا، أو أن نشهد حالات زواج بين البشر والرُّبوتس؟!!

وتكمن أهمية وضع قواعد أخلاقية - وأيضًا قانونية - تحكم الذَّكاء الاصطناعي في أنه مصمم للقيام بوظائف مفيدة للبشرية، وسيقوم بها، بغض النظر عن الظروف المحيطة أو المستجدة، فمثلًا إذا قام أحد الأطفال في المنزل بمحاولة إعاقة الرُّوبوت عن القيام بوظائفه في تنظيف المنزل على سبيل الدعابة، فإن الرُّوبوت سيتعامل مع هذا الموقف باعتباره تهديدًا يعوقه عن القيام بوظيفته، وقد يتسبب في مقتل هذا الطفل من أجل القيام بوظيفته التي صمم من أجلها، أسئلة وقضايا أخلاقية وفلسفية كثيرة، لا بد من الإجابة عنها أولًا لضمان الحفاظ على هويتنا البشرية.

ومن هنا لا بد من الاهتمام بإنشاء آلية تنظيمية وأخلاقية تحكم عمل الذَّكاء الاصطناعي، وحماية الوظائف التي سوف تتأثر من جراء هذه الأئتمة الذَّكيَّة، وصياغة قوانين تضمن الحفاظ على حقوق البشر الأساسية، مع تشجيع الابتكار في مجال الذَّكاء الاصطناعي الصديق للإنسان، ووضع منظومة قيمية تحكم العلاقة بين الإنسان والآلة في عصر قد تتفوق فيه الآلة على الإنسان.

ثانيًا: إنترنت الأشياء

يُعَدُّ «إنترنت الأشياء» أحد أسرع القطاعات التكنولوجية نموًّا في العالم، ويُقصد به «تهيئة جميع الأجهزة والأدوات المحيطة بنا لتصبح متصلة بالإنترنت، مثل الأدوات الكهربائية، وقطع الأثاث، والألعاب الإلكترونية، والسيارات، والساعات، والنظارات، والملابس، والأحذية، وغيرها من مليارات الأجهزة والأدوات، وأن تتمكن من الاتصال ببعضها البعض بصورة آلية وفورية دون الحاجة إلى تدخل الإنسان، وأن تتبادل المعلومات فيما بينها، وتتخذ القرارات الملائمة في الوقت المناسب»، وبذلك تصبح جميع الوحدات التي يعمل البشر في إطارها، سواء كانت منازل، أو مدنًا، أو مصانع، وشركات، ومزارع، بل وحتى الأفراد أنفسهم، أكثر ذكاءً.

وبصورة عامة، يُقصد بإنترنت الأشياء أيضًا «أي ارتباط يجمع الأشياء المادية حولنا بشبكة الإنترنت، بحيث يمكن معرفة معلومات دقيقة عن حالتها، والتحكم فيها في أي وقت وفي أي مكان». ولكي يتحقق ذلك لا بد من توفر ثلاثة مكونات رئيسية، هي شبكة إنترنت، وشيء مادي متصل بالشبكة، وبرنامج يقوم بعملية التحكم في الأشياء المادية، سواء بصورة آلية أو من خلال تحكم إنساني عن بُعد. وقد وفرت التكنولوجيا الحديثة، خاصة في عالم الاتصالات والهواتف الذَّكيَّة، هذه الثلاثية، التي سخرت عديدًا من الأجهزة الإلكترونية والمادية، من خلال التَّطبيقات الذَّكيَّة؛ فالإنترنت هو بمثابة الروح التي يتم بثها في الأجهزة الصماء، لكي ترى، وتسمع، وتسجل، وتتواصل، وتتفاعل، من خلال برمجيات وخوارزميات تحكم عملها.

1- تطبيقات إنترنت الأشياء:

تتعدد تطبيقات إنترنت الأشياء في مجالات متنوعة تمس حياة الأفراد بشكل يومي، سواءً في المنزل، أو في العمل، أو حتى الميدان الاقتصادي والصناعي. وقد ظهر في هذا الإطار عدد من الأمثلة تنوعت في مجالات مختلفة، فمنها ما ظهر في مجال الأجهزة المنزلية كما في تطبيق «نيست» الذي يعمل كمنظم للحرارة، ويتحكم في درجة التدفئة، وتطبيق «جود نايت لامب» الذي يتحكم في تشغيل المصابيح الكهربائية، و»فيول باند» لتعقب حركة الفرد أينما ذهب، والذي أطلقته شركة نايك، فضلًا عن تطبيقات أخرى في مجال ترشيد المياه والكهرباء عن بُعد، والتي أطلقتها شركة «بوش» إحدى أهم الشركات المبتكرة لتطبيقات إنترنت الأشياء[1].

ولا تقف أمثلة هذه النماذج عند تطبيقات الأجهزة المنزلية فقط، لكنها تجاوزت مداها حتى وصلت إلى تطبيقات الملابس القابلة للارتداء، والتي تسمح بإرسال ومعالجة البيانات عبر تطبيقات الهاتف المحمول[2]. ومن الأمثلة الشائعة التي لقيت رواجًا كبيرًا في الفترة الأخيرة تطبيق الساعات الذَّكيَّة، والتي زاد معدل الطلب عليها كثيرًا منذ عام 2015، وظهور القميص المتصل The Pole Tech Shirt كتطور جديد في عالم إنترنت الأشياء، والذي يساعد في تحديد المسافات وحرق السُّعرات الحرارية وقياس معدل ضربات القلب[3].

وتنتشر تطبيقات إنترنت الأشياء في المجال الصناعي، والذي عكست تطبيقاته نتائج مُذهلة، فقد ساعد إنترنت الأشياء في مجال توفير مبالغ طائلة

1- تواصل مع حياتك اليومية بإنترنت الأشياء.. ستة مليارات قطعة ستكون موصولة بالشبكة الإلكترونية خلال عامين، جريدة الشرق الأوسط، يوليو 2013، للمطالعة: https://bit.ly/2BQftMd.

2- The M2M, IoT & Wearable Technology Ecosystem: 2015 - 2020 - Opportunities, Challenges, Strategies, Industry Verticals and Forecasts, September 2016. On https://prn.to/2RgZnF8

3- 2015 Wearable Tech Trends: Swank Meets Science, available on :http://www.itbusinessedge.com/slideshows/2015-wearable-tech-trends-swank-meets-science-06.html.

في قطاع الصناعة، حيث نجحت شركة «إنتل» في توفير مبالغ مالية وصلت إلى 9 ملايين دولار في فروعها بماليزيا، وذلك من خلال تحسين أداء عمل الآلات عبر إنترنت الأشياء وتقليل معدلات الخطأ[1].

ويُضاف إلى ذلك مجالات تطبيقية أخرى، مثل برامج رصد حركة الاختناقات المرورية، ورصد أوضاع الطيران والتنقل بالسكك الحديدية وغيرها[2]، كما يظهر تطبيق إنترنت الأشياء في مجالات أخرى، مثل التعدين، حيث وفرت شركة «ريو تينتو» مبالغ طائلة وصلت إلى 300 مليون دولار من جراء استخدامها إنترنت الأشياء، كما وفرت كل من شركتي «أجريوم»، و«دوبونت» الأوروبيتين 20 مليون دولار بفضل تطبيقهما قوة إنترنت الأشياء في المجال الزراعي[3].

2- التحديات التي يطرحها إنترنت الأشياء:

ليس هناك شك في أن المميزات التي سيحصل عليها الأفراد من إنترنت الأشياء عديدة ومتنوعة، والاعتماد على إنترنت الأشياء في القطاع الصناعي من شأنه المساعدة في تحقيق وفورات مالية كبرى للشركات، فضلًا عن تحقيق أقصى استفادة في مجال إدارة الموارد، لا سيما الموارد المائية والكهربائية وترشيد استخدامهما، ولكن مخاطر إنترنت الأشياء لا يمكن تجاهلها، أو غض النظر عنها، خاصة إذا كانت تؤثر على أمن الأفراد وحياتهم الشخصية. **ومن أبرز التحديات الناجمة عن إنترنت الأشياء ما يلي:**

1- Rich Quinnell , Industrial Internet of Things Is On Its Way, 2-Jan-2015, available on : http://www.eetimes.com/
author.asp? section_id=36&doc_id=1325140
2- Cyber-Physical Systems Driving force for innovation in mobility, health, energy and production, OP. Cit, p:10.
3- Menno van Doorn, Morgan Stanley Reports on Internet of Things Disruptions, available on: http ://labs.sogeti.com/morgan-stanley-reports-internet-things-disruptions

أ- اختراق الخصوصية والانكشاف المتزايد للأفراد والمؤسسات:

تهتم كثير من الشركات بتطوير منتجاتها التقليدية لتكون متصلة بالإنترنت، وإتاحة إمكانية التحكم فيها من خلال الهواتف الذَّكيَّة، دون أن تهتم بتأمين هذه المنتجات؛ فعلى سبيل المثال تهتم الشركات المنتجة للقهوة بأن تجعل ماكيناتها ذكية في تقديم القهوة، لأن الهدف هنا هو القهوة بالأساس، ولكنها تغفل - بقصد أو من دون قصد - عن تأمين الجهاز نفسه من الاختراق الخارجي.

وطالما ستكون هذه الأجهزة في كل الأماكن، في المنازل والمطاعم والمؤسسات والشوارع، فإن اختراقها يهدد خصوصية البشرية، فالجميع سيكون منكشفًا على الجميع، وتكون التداعيات أكبر عند الحديث عن الخصوصية الشخصية، خاصة مع وجود اتجاه متصاعد للاستثمار في المنازل الذَّكيَّة التي تقوم فكرة عملها على شبكة لا سلكية تتصل بها جميع الأجهزة المنزلية، ويتم التحكم فيها من خلال الهواتف الذَّكيَّة[1].

ب- التلاعب بالأجهزة واستخدامها كوسيط لاختراق أجهزة مُؤَمَّنة:

إذا ما لم تكن الأجهزة قوية التأمين من الاختراق، فإنه يسهل الوصول إليها والتلاعب بها من أطراف خارجية تقوم بعملية التحكم عن بُعد، بحيث تدفع هذه الأجهزة إلى القيام بمهام غير مهامها الرئيسية، أو حتى التلاعب بمهامها الأساسية، وفصل سيادة أصحابها وسيطرتهم عليها، والتسبب في خسائر فادحة؛ فإذا كان هذا الجهاز مثلًا سيارة ذاتية القيادة، فإن اختراقها قد يترتب عليها مقتل الشخص الذي بداخل السيارة، وتكون الخسائر مماثلة عند الحديث عن التلاعب بالأجهزة والمعدات الطبية التي تحدد الحالة الصحية للمرضى، فالتلاعب بالبيانات التي تظهر للأطباء قد يؤدي إلى وفاة المريض.

1- The Case for the Intranet of Things and the Smart Home, June, 2013, available on : http://www.qtooth.com/the-intranet-of-things-and-the-smart-home

ولا يقتصر الأمر على ذلك فقط، بل قد يشمل استخدام هذه الأجهزة كوسيط للسيطرة على أجهزة أخرى، مثل استخدام أحد الأجهزة المتصلة بالإنترنت كالساعات الذَّكيَّة التي يرتديها أحد الموظفين للسيطرة على خوادم إحدى الشركات أو البنوك والمؤسسات، أو العبث بشبكات الطاقة والمولدات والسدود وغيرها من البنية التحتية الحرجة.

ج- إدارة المعلومات العملاقة الناجمة عن تواصل الآلات:

إن إحدى القدرات التي تميز إنترنت الأشياء هي قدرة الآلات على التواصل مع بعضها البعض Machine To Machine Communication، ولكن يظهر التحدي في هذا المجال في حالة زيادة حجم البيانات والمعلومات نتيجة التزايد المتوقع في حجم مستخدمي إنترنت الأشياء، والتي يتوقع أن تتجه المنظمات نحو حتمية التعامل مع هذه المشكلة من خلال تجميع البيانات في مراكز صغيرة موزعة بحيث يمكن من خلالها معالجة البيانات والمعلومات[1].

> يخلق ارتباط الأشياء المادية حولنا بشبكة الإنترنت، وإمكانية التحكم فيها في أي وقت وفي أي مكان، علاوة على قدرة الآلات على التواصل مع بعضها البعض؛ تحديات عديدة، يتمثل أبرزها في: كيفية التعاملً مع حجم البيانات الضخمة، ومع الزيادة المُضاعفة في عدد مستخدمي إنترنت الأشياء، ومع حماية الخصوصيات الشخصية، ومع عمليات تأمين الأجهزة من الاختراق أو التلاعب بها من أطراف خارجية تحاول التحكم فيها عن بُعد لأهداف مختلفة.

وبالتالي، يجب أن تتعامل الدول بحذر مع إنترنت الأشياء، دون تقييد عملية التطوير والتحديث، ودون أن تعزل نفسها أيضًا عن واحد من أهم مُحرِّكات التقدم البشري في مجال التكنولوجيا،

1- Matthew Finnegan,Internet of Things will disrupt data centre management, says Gartner 26 billion connected devices by 2020, Computer World Uk, March 19, 2014: https://bit.ly/2Rq9Kqa

وأن تستفيد من المميزات المتعددة التي تترتب على استخدام إنترنت الأشياء في القطاعات المختلفة، مثل تحسين أداء عمل المؤسسات وتحقيق وفورات مالية من تحديث نظم الصناعات وغيرها، مع تجنب التداعيات السلبية الناجمة عن استخدام إنترنت الأشياء، وذلك من خلال وضع معايير قياسية للأجهزة المسموح بدخولها للدولة، وتنظيم عملية استخدامها في الأماكن ذات الحساسية العالية كالمؤسسات المالية والأمنية، والبنى التحتية الحرجة، وزيادة القدرات الشرطية في مجال تحقيق الأدلة الجنائية الرقمية وتتبع الهجمات السيبرانية، وتشجيع عملية تأمين منتجات إنترنت الأشياء؛ بما يخلق بيئة سيبرانية آمنة لجميع المستخدمين.

ثالثًا: سلسلة الكُتلة «البلوك تشين»

البلوك تشين، أو سلسلة الكُتلة، هي الجيل الجديد من الإنترنت الذي يسمح بنقل أصل الملكية من طرف إلى آخر في نفس التوقيت، ودون الحاجة إلى وسيط مع تحقيق أقصى درجات الأمان، وهي أيضًا «السجل» العالمي الموزع بين جميع الأفراد حول العالم ويضمن لهم إجراء معاملتهم[1]، أيًّا كانت هذه المعاملة، في الوقت الحقيقي لها، مع ضمان صحة المعاملة وعدم الغش أو التلاعب بها، وهي أيضًا أكبر قاعدة بيانات موزعة عالميًّا بين الأفراد[2] تحتوي على أصول موثقة لهم تسمح بتبادلها بينهم بدرجة ثقة عالية.

وتم استخدام نظام البلوك تشين، أو سلسلة الكُتلة، لأول مرَّة في عام 2008، أي منذ أكثر من عشر سنوات، وذلك باعتباره المنصة الرئيسية لعملة البيتكوين الافتراضية، تلك العملة التي استمدت قوتها وثقة المتعاملين فيها، على الأقل حتى الآن، بفضل ذلك النظام. وعلى الرغم من ذلك، فإن كثيرين يخلطون ما بين البيتكوين، والبلوك تشين، ويعتبرون أن كليهما واحد؛ وهو أمر غير حقيقي، فالبلوك تشين هو العمود الفقري لعملة البيتكوين، وهو ما يميزها عن غيرها من العُملات الافتراضية الأخرى[3]، ومثلما تم استخدامه في تحويل العُملات الافتراضية، يمكن أيضًا استخدامه في مئات التَّطبيقات الأخرى.

ولكي يمكن نقل أصل الشيء أو إجراء معاملة من طرف إلى آخر، لا بد من الذهاب إلى وسيط، سواء كان بنكًا لتحويل النقود، أو وزارة حكومية لتوثيق المعاملة، أو شهرًا عقاريًّا لإثبات الملكية، أو سمسارًا لشراء عقار، أو خلافه، ودائمًا ما يقوم هذا الوسيط بتحصيل نسبة من المعاملة كرسوم أو أجر للقيام

1 -BlockChain Technology, Sutardja Center for Entrepreneurship & Technology Technical Report, Brekely University of California, October 16, 2015, p1
2- A Scalable Blockchain Database,BigchainDB, Berlin, Germany, June 8, 2016, p1
3- An Introduction to Bitcoin and Blockchain Technology, KAYE Scholar, February 2016, accessed Feb 10, 2018, on: https://bit.ly/2oIoDnV

بمهام الوساطة الموثوقة... لكن مع تقنية سلسلة الكُتلة، أو البلوك تشين، سيتم إجراء المعاملة أو نقل أصل الملف إلى الطرف الآخر وتخزينه وإدارته دون أن تكون هناك حاجة إلى هذا الوسيط، أو أن الوسيط الحقيقي في هذه الحالة سيكون ملايين أجهزة الحواسب الأخرى المتصلة بالسلسلة، والتي تنتقل بينها المعاملة بصورة مشفرة وآمنة وموثَّقة حتى تصل إلى الطرف الآخر، مع الاحتفاظ بإمكانية عدم التلاعب أو التزوير أثناء إجراء المعاملة، وضمان حق الأولوية في التسجيل، وهو ما يعني بصورة مباشرة تهديد ملايين الوظائف حول العالم.

وما يعجل نظام «البلوك تشين» أحد المُحرِّكات الجوهرية للثورة الذَّكيَّة التي تشهدها الحياة البشرية ويجعل منه إحدى أهم أدوات إدارة حياة الأفراد، توافر ميزتين رئيسيتين له، وهما:

الميزة الأولى: نقل أصل الملفات: فالهدف الرئيسي من البلوك تشين هو نقل أصل الشيء إلى الطرف الآخر عبر شبكة الإنترنت، فما يحدث دائمًا هو نقل نسخة من الملف وليس نقل الملف الأصلي، بمعنى أنه عند إرسال إيميل أو ملف عبر الإنترنت، فإن ما يحدث هو إرسال نسخة من الملف أو المعلومات الموجودة عن الطرف الأول إلى الطرف الثاني، مع إمكانية الطرف الأول بالاحتفاظ بالأصل، وهو ما لا يمكن أن يحدث عند محاولة نقل أصل الشيء مثل الأموال، فلا يمكن أن تقوم بإرسال مبلغ مئة دولار لأحد الأفراد ثم تحتفظ به مرَّة أخرى لنفسك. وكذلك الأمر ينطبق على التصويت في العملية الانتخابية، والحصول على حقوق الملكية الفكرية وبراءات الاختراع، أو شراء الملفات الأصلية كالأغاني والأفلام الأصلية التي يتم شراؤها والاستحواذ عليها بصورة نهائية، بما يعني أنه لا ينبغي لطرف آخر الاحتفاظ بها[1].

1- Don Tapscott, How the blockchain is changing money and Business, TED Summit, June 2016, Accessed Feb 5, 2018, on: https://bit.ly/2bp4XiI

الميزة الثانية: عدم إمكانية التلاعب، فالخاصية الأبرز التي تميز «البلوك تشين» هي عدم الغش أو التدليس أثناء تنفيذ المعاملات التي يتم إجراؤها عبر البلوك تشين، وعدم التلاعب بالمعاملات بعد إتمامها. وهذا ينطبق على عديد من الأنشطة اليومية، مثل عمليات نقل الأموال والطرود، والشحنات، والحاويات، وعمليات تسجيل العقود والممتلكات وشحن البضائع، والتأكد من خط سير المركبات والمواصلات، وإجراء المعاملات الحكومية؛ حيث تمنع البلوك تشين التلاعب بالمعاملات بصورة تسبب الإضرار بثروات الدولة أو الإخلال بمبدأ تكافؤ الفرص؛ وهو ما يساعد في القضاء على الفساد بصورة كبيرة، حيث يضمن نظام البلوك تشين عدم التلاعب بها وعدم التعديل عليها أو حذفها لاحقًا، وهو ما يساعد في خلق الثقة بين المستخدمين بصورة كبيرة[1].

1- مبادئ نظام البلوك تشين:

يعمل نظام البلوك تشين وفق ثلاثة مبادئ رئيسية، تمثل الأساس الذي يقوم عليه هذا النظام، **ويتم في إطاره إنجاز جميع معاملات الأفراد، وهي:**

أ - السجل المفتوح Open Ledger:

يعني ذلك أن جميع المعلومات الموجودة داخل البلوك تشين متاحة للجميع، حيث يرى جميع الأفراد الموجودين داخل السلسلة ممتلكات بعضهم البعض، فمثلًا إذا كانت هذه السلسلة خاصة بتحويل أموال، يستطيع كل من بالسلسلة رؤية أموال الجميع، لكن مع الاحتفاظ بعدم القدرة على معرفة هويتهم الحقيقية، وذلك لأن السلسلة تتيح للأفراد إمكانية استخدام ألقاب Nick Names تظهر لمستخدمي السلسلة؛ وبالتالي يصعب التعرف على هوية الشخص، لكن يسهل معرفة ما معه من أموال[2].

1-BlockChain Technology, Ob cit, p5
2- Marco Iansiti and Karim R. Lakhani,The Truth About Blockchain, Harvard Business Review, Jan-

ومثال على ذلك، إذا أراد الشخص (أ) تحويل مبلغ 10 دولارات إلى الشخص (ب)، فإنه يظهر للجميع عما إذا كان هذا الشخص بالفعل يمتلك عشرة دولارات أم لا، وفي حالة عدم امتلاكها تصبح المعاملة غير صحيحة ولا يتجاوب أحد معها بالتحويل، أما إذا كانت صحيحة فإن أقرب شخص موجود بجوار الشخص (ب)، وليكن اسمه (ج)، يقوم بإعطاء النقود للشخص (ب) مقابل نسبة صغيرة يأخذها من المبلغ الإجمالي الذي يريد الشخص (أ) إرساله.

ويعتبر العيب الرئيسي في هذا المبدأ هو إمكانية معرفة معلومات شخصية عن بعض الأفراد، مثل أن رب أسرة يقوم بتحويل أموال لأسرته، فمن خلال السجل الخاص به يمكن معرفة حجم أمواله على السلسلة، والأشخاص الذين يقوم بتحويل الأموال إليهم من عائلته مثل زوجته وأبنائه، والتوقيتات التي يقوم فيها بعملية التحويل، وهذه المعلومات يمكن توظيفها فيما بعد للتدبير لعمل جنائي أو إجرامي ضد أفراد الأسرة.

ب- قاعدة البيانات الموزعة Distributed Database:

الهدف الرئيسي من هذا المبدأ هو القضاء على فكرة المركزية، حيث لا توجد جهة واحدة أو خادم Server واحد أو جهاز واحد يتحكم في سلسلة الكُتلة، بل إن السلسلة موزعة بين جميع الأفراد المشتركين فيها حول العالم، حيث يمكن لأي شخص في العالم أن يقوم بتحميل السلسلة والاطلاع عليها والمشاركة فيها.

ويُعتبر هذا المبدأ أحد عناصر الأمان للسلسلة، فإذا أراد أحد القراصنة التلاعب بالسلسلة أو اختراقها، فلا بد له أن يخترق جميع الأفراد الموجودين بها[1].

uary–February 2017 ISSUE, https://hbr.org/2017/01/the-truth-about-blockchain
1 -ibid

ج- التنقيب Mining:

يعني هذا المبدأ اشتراك ملايين الأجهزة حول العالم في التأكد من صحة المعاملة قبل إتمامها، فإذا أراد أحد الأفراد تحويل مبلغ نقدي لآخر عبر السلسلة، فإن المعاملة لا تتم حتى وإن كان الشخص يمتلك بالفعل هذه النقود حتى تحدث عليها عملية التنقيب.

ويُقصد بعملية التعدين أو «التنقيب» استخدام طاقات أجهزة الكمبيوتر في البحث عن «الهاش» الصحيح المميز لهذه المعاملة حتى تتم بنجاح»، حيث يقوم ملايين من المنقبين Miners حول العالم بإجراء مجموعة من العمليات الحسابية المعقدة عبر أجهزتهم بغرض الحصول على «الهاش» الصحيح الذي يربط هذه المعاملة بالمعاملة السابقة لها داخل السلسلة ويميزها عن غيرها من المعاملات الأخرى التي تتم داخل سلسلة الكُتلة.

وتُعتبر هذه هي الوظيفة الرئيسية لعملية التعدين، أي التأكد من أن جميع المعاملات التي دخلت السلسلة أخذت الوقت نفسه الذي أخذته المعاملة الجديدة[1]. وبمجرد أن يتم الحصول على «الهاش» الصحيح يتم إتمام المعاملة والسماح لها بالدخول في السلسلة، ويتم ضمها إلى غيرها من العمليات داخل الكتل المكونة في النهاية لسلسلة الكُتلة[2]، وهو ما يجعل عملية اختراق النظام أو التلاعب به أمرًا صعبًا للغاية لأنه يتطلب اختراق جميع هذه الأجهزة في الوقت نفسه. وهنا يمكن إتمام المعاملة بعد التأكد من صحتها، ويفوز المنقب الذي حصل على «الهاش» الصحيح على نسبة من عملية التحويل، فإذا كان الأمر نقل عملة البيتكوين مثلًا، فإنه يحصل على مكافأة مقابل عملية التنقيب.

1- Six myths about blockchain and Bitcoin: Debunking the effectiveness of the technology, Kaspersky, August 18, 2017https://www.kaspersky.com/blog/bitcoin-blockchain-issues/18019/
2- Blockchain – Distributed Ledger Technology Application Benefits?, bitcoinexchangeguide, Accessed Feb 4, 2018 on https://bitcoinexchangeguide.com/blockchain-distributed-ledger-technology/

2- عناصر نظام البلوك تشين:

يتكون أي نظام بلوك تشين من أربعة عناصر رئيسية هي: الكُتلة، وتمثل وحدة بناء السلسلة، والمعلومة، والهاش، وبصمة الوقت. **ويمكن توضيح ذلك كما يلي:**

أ- الكُتلة:

تمثل مجموعة من العمليات أو المهام المرجو القيام بها أو تنفيذها داخل السلسة. ومن أمثلة الكتل Blocks تحويل أموال، أو تسجيل بيانات، أو متابعة حالة... إلخ. وعادة ما تستوعب كل كتلة مقدارًا محددًا من العمليات والمعلومات لا تقبل أكثر منه حتى يتم إنجاز العمليات بداخله بصورة نهائية، ثم يتم إنشاء كتلة جديدة مرتبطة بها. والهدف الرئيسي هو منع إجراء معاملات وهمية داخل الكُتلة تتسبب في تجميد السلسلة أو منعها عن تسجيل وإنهاء المعاملات.

ب- المعلومة:

هي العملية الفرعية التي تتم داخل الكُتلة الواحدة، أو هي الأمر المفرد Single Order الذي يتم داخل الكُتلة، ويمثل مع غيره من الأوامر والمعلومات الكُتلة نفسها.

ج- الهاش Hash:

هو عبارة عن الحمض النووي المميز لسلسلة الكُتلة، ويرمز إليه البعض أحيانًا بالتوقع الرقمي Digital Signature، أي إنه كود يتم إنتاجه من خلال خوارزمية داخل برنامج سلسلة الكُتلة يطلق عليها «Hash Function»، أو آلية الهاش[1]، ويقوم بأربع وظائف رئيسية: أولها تمييز السلسلة عن غيرها من السلاسل، حيث تحصل كل سلسلة على «هاش» مميز لها وخاص بها، وثانيها تمييز

1- Stephen Northcutt, Hash Functions, SANS™ Technology Institute, Accessed Feb 6, 2018 on https://www.sans.edu/cyber-research/security-laboratory/article/hash-functions

كل كتلة عن غيرها داخل السلسلة، حيث تأخذ كل كتلة أيضًا «هاش» خاصًّا بها ومميزًا لها، وثالثها تمييز كل معلومة داخل الكُتلة نفسها بهاش مميز لها، ورابعها ربط الكتل بعضها البعض داخل السلسلة، حيث ترتبط كل كتلة بالهاش السابق لها وبالهاش اللاحق لها، مما يجعل الهاش يسير في اتجاه واحد فقط من الكُتلة الأصلية للاحقة عليها، وهكذا، لذلك لا يسمح الهاش بالتعديل على الكتل التي تم إنشاؤها.

د- بصمة الوقت:

هو التوقيت الذي تم فيه إجراء أي عملية داخل السلسلة[1].

3- تطبيقات استخدام البلوك تشين:

تتعدد استخدامات البلوك تشين في عدة مجالات مختلفة، لا تقتصر فقط على تحويل الأموال، سواءً كانت افتراضية، أو تقليدية. **ويمكن توضيح ذلك في الآتي:**

أ- تسجيل الممتلكات:

تتمثل إحدى وظائف نظام البلوك تشين في قدرة الأفراد على تسجيل ممتلكاتهم، أيًّا كانت هذه الممتلكات، سواء كانت عقارات، وأراضيَ، أو مجوهرات وأحجارًا كريمة، أو سيارات وممتلكات شخصية، أو براءات اختراع وحقوق ملكية فكرية، كالكتب، والأغاني، والأشعار، بل وحتى مجرد الأفكار العادية التي لم ترتقِ لاختراع أو إنجاز بشري، أو غيرها، مما يمتلكه الأفراد ويرغبون في الإعلان عنه أو تسجيله لضمان حقوقهم، بحيث يستطيع الأفراد بعد ذلك بيعها عبر نظام البلوك تشين، أو إجراء معاملات عليها فيما بعد[2].

1- Luke Parker, Timestamping On The Blockchain, bravenewcoin, 11 Feb 2015, accessed Feb6, 2018, on: https://bravenewcoin.com/news/timestamping-on-the-blockchain/
2- EYAL MALINGER,Blockchain could 'change everything' for real estate, venturebeat, https://venturebeat.com/2017/11/18/blockchain-could-change-everything-for-real-estate/

ب- تسجيل المعاملات:

يُقصد بها أي معاملة، سواءً كانت شخصية بين الأفراد أو داخل شركة أو مؤسسة حكومية أو غير حكومية، فنظام البلوك تشين هو بمثابة سجل رقمي مفتوح وموزع، يسمح للجميع إدخال جميع البيانات عليه، سواءً كانت هذه البيانات إجراءات حكومية[1]، أو متابعة خطوط الإنتاج في مصنع، أو خط سير طائرات أو حاملات النفط، فضلًا عن تسجيل معاملات البيع والشراء ونقل الملكيات ومتابعة خدمة العملاء وتسجيل جميع المعاملات التي تمت بين أي فردين في أي مجال، بما يتيح اكتشاف الثغرات ومكافحة الفساد ومُراقبة الجودة.

تتعدد مميزات نظام "البلوك تشين" أو "سلسلة الكتلة" باعتبارها تشكل جيلًا جديدًا من الإنترنت واستخداماته؛ فهو بمثابة نظام إداري ومالي قادر على القيام بعدة وظائف حقيقية، مع توفير أكبر قدر من الوقت والجهد والتكلفة الحقيقية للقيام بالمهام، مع القدرة على مراقبة جميع العمليات والتأكد من مصدرها، بالإضافة إلى عدم القدرة على الغش أو التزوير أو التلاعب.

ج- أعمال الوساطة:

تقوم البلوك تشين بإحلال الوسيط الموجود أثناء تقديم الخدمة، فتحل محل البنوك في تحويل الأموال، ومحل الشهر العقاري في تسجيل الممتلكات، ومحل إدارات المرور في تسجيل السيارات، ومحل السماسرة في عمليات البيع والشراء، ومحل الشركات الوسيطة، مثل «أوبر» في تقديم الخدمات، وذلك لصالح وسيط جديد، هو ملايين الأفراد حول العالم الذين يستخدمون السلسلة ويستفيدون من العائد المادي الذي كان يعود على الوسيط التقليدي، وعلى الرغم من ضآلة هذا العائد، فإنه قد يحقق مبدأ العدالة في توزيع الثَّورة بين الأفراد.

1- An Analysis of the Opportunities and Threats in Blockchain Technology, MEDIUM, Feb 13, 2017, accessed Feb 15, 2018, on: https://medium.com/the-mission/an-analysis-of-the-opportunities-and-threats-in-blockchain-technology-6f55d647be3e

4- المميزات التي تحققها البلوك تشين:

تتعدد المميزات التي تقدمها البلوك تشين، فهي نظام إداري ومالي قادر على القيام بعدة وظائف حقيقية مع توفير أكبر قدر من الوقت والجهد والتكلفة الحقيقية للقيام بالمهام، مع القدرة في الوقت نفسه على مُراقبة جميع العمليات والتأكد من مصدرها، بالإضافة إلى عدم القدرة على الغش أو التزوير أو التلاعب فيها بفضل آلية الهاش. **ومن المميزات التي يحققها هذا النظام ما يلي:**

أ- التخلص من أعباء الروتين:

يساعد هذا النظام الدوائر الحكومية على تحقيق الفاعلية، فجميع المعاملات الخاصة بالأفراد يمكن أن تكون واضحة داخل السلسلة، وإذا كان هناك حاجة للتأكد من بعض المعلومات أو الشهادات أو الوثائق يمكن بسهولة الاطلاع عليها، مما يساعد في توفير الوقت والقضاء على الروتين[1].

ب- ضمان تحقيق الجودة:

يسمح نظام البلوك تشين بتتبع جميع الخطوات الخاصة بالمعاملة، وهو ما يساعد في النهاية على ضمان تقديم الخدمة بأفضل جودة ممكنة، فمثلًا إذا كان هناك خط إنتاج أحد الأطعمة فإن النظام يضمن جودة المنتجات النهائية[2].

ج- القضاء على الفساد:

لا يسمح نظام البلوك بالتعديل أو الإلغاء، فجميع المعاملات التي تتم عليه مسجلة خطوة بخطوة بالتوقيت، وفي حالة التلاعب أو التزوير لا تقبل السلسلة إدخال المعاملة مرَّة أخرى، بما يساعد في القضاء على الفساد.

1- Sean Williams, 5 Big Advantages of Blockchain, and 1 Reason to Be Very Worried, Fool, Dec 11, 2017, accessed Feb 15,2018 on https://bit.ly/2EBam6n
2- Jyoti Agrawal, 8 Benefits of Blockchain to Industries Beyond Cryptocurrency, entrepreneur, accessed Feb 15, 2018, on: https://bit.ly/2mI7tVQ

د- التوزيع العادل للثروة:

يساهم هذا النظام في توزيع الثَّروة بين جميع الأفراد حول العالم وعدم احتكارها من قبل بعض الهيئات أو المنظمات، وذلك لأن جميع الأفراد حول العالم يمكن أن يتشاركوا في إنهاء المعاملات والحصول على نسبة منها.

5- سلبيات البلوك تشين:

على الرغم من المميزات التي يقدمها نظام البلوك تشين؛ فإن هناك عددًا من التخوفات والتهديدات المستقبلية التي يطرحها هذا النظام، ولعل من أهمها وأخطرها ما يلي:

أ- احتمال القضاء على القطاعات والوظائف الوسيطة:

يُعتبر التهديد الأكبر الذي يطرحه نظام البلوك تشين لدى قطاعات المال والإدارة والأعمال الوسيطة، والتي من المتوقع أن يكتب لها هذا النظام الفناء والاندثار كما فعلت التطورات التكنولوجية في كثير من الصناعات والأعمال والحرف من قبل، إلا إذا استطاعت هذه الوظائف تطوير نفسها لاستيعاب هذه التقنية الجديدة[1].

ب- استخدام البلوك تشين في أعمال غير قانونية:

قد تكرس البلوك تشين تجارة المخدرات والبغاء والسلع الممنوعة والأسلحة، وهو ما يهدد السلم المُجتمعي ويضر بمصالح الأفراد.

1- Monica Eaton-Cardone, How blockchain will affect financial services employment, Efinancialcareers, 4 January 2017, accessed Feb 13, 2018 on:
https://bit.ly/2GOC7tY

ج- إمكانية سرقة البيانات الشخصية للأفراد:

يمكن سرقة البيانات الخاصة بالأفراد عبر الدخول إلى السلسلة، والتمكن من التلاعب بممتلكاتهم أو بيعها أو الإضرار بوظائفهم أو غيرها من المخاطر.

د- إمكانية الاختراق والتعرض لهجمات منع الخدمة:

يمكن أن تظهر هجمات منع الخدمة على الرغم من تصميم النظام القائم على منع مثل هذه الهجمات من خلال تحديد حجم البلوكات، ولكن يظل هناك احتمال قائم أيضًا يتسبب في إيقاف السلسلة عن العمل نتيجة التعرض لهجوم إلكتروني[1].

وعلى الرغم أيضًا من أن اختراق السلسلة صعب إلى حد كبير، لأنه يتطلب اختراق جميع الموجودين بالسلسلة ومن يقوم بعملية التنقيب، فإنه احتمال وارد في السلاسل قليلة العدد من حيث الاستخدام، ومن حيث المنقبين.

6- التداعيات المترتبة على استخدام البلوك تشين:

من شأن البلوك تشين أن تهدد أدوار جميع المؤسسات التقليدية، بدءًا من الحكومات والمؤسسات البيروقراطية، مرورًا بالشركات والمؤسسات المالية والوسيطة، وانتهاءً بالنظم السياسية والتشريعات القانونية التي اعتادت عليها البشرية، وهو ما يدفع هذه المؤسسات إلى ضرورة إعادة تقييم التداعيات التي سوف تترتب عليها جراء انتشار هذه التقنية لكي تتطور وتتكيف مع الواقع التكنولوجي الجديد.

1- An Analysis of the Opportunities and Threats in Blockchain Technology, MEDIUM, Feb 13, 2017, accessed Feb 15, 2018, on: https://bit.ly/2TbH0ys

وبصورة عامة، **يمكن تحديد أبرز التداعيات المترتبة على البلوك تشين في التالي:**

أ- التداعيات السياسية:

يتيح نظام البلوك تشين للأفراد تكوين كتل بشرية افتراضية موثوق في صحتها وبياناتها، وتستطيع هذه الكتل أن تفرض رغبتها حيال كثير من الأمور، فتعود بنا إلى فكرة «ديمقراطية المدينة»، تلك الديمقراطية التي يشارك فيها جميع أفراد المُجتمع في اتخاذ القرارات، فإذا كانت الدولة بصدد إجراء تعديل دستوري أو إصدار قانون تشريعي أو إجراء استفتاء حول بعض القضايا التي تهم المواطنين، أو حتى إجراء انتخابات نيابية أو رئاسية، فيمكن في هذه الحالة مشاركة جميع أفراد الدولة، سواءً كانوا داخلها أو خارجها، بصورة مباشرة دون الحاجة إلى وجود مجلس نيابي عنهم، وذلك عبر سلسلة الكُتلة.

سوف يثير انتشار نظام "البلوك تشين" بعد مرور سنوات قليلة تداعياتٍ خطيرة، من أبرزها أنه سوف يهدد بشكل ما الأدوار التقليدية للمؤسسات التقليدية، الحكومية وغير الحكومية، سواءً الاقتصادية مثل البنوك والمؤسسات الوسيطة، أو السياسية مثل البرلمان ذاته؛ وذلك لأن هذا النظام سوف يُتيح للجميع المشاركة المباشرة في عملية اتخاذ القرارات، وربما يمكنه تطبيق فكرة "ديمقراطية المدينة"، خاصة في المجتمعات القليلة العدد والأكثر استخدامًا للتكنولوجيا.

ويهدد مثل هذا الأمر دور البرلمان بصورة كبيرة، وذلك لتوفر أداة للمُجتمع يمكن من خلالها القيام بحقوقه الأصلية دون الحاجة إلى نواب عنه، حيث يمكن لجميع الأفراد المشاركة في مُراقبة أداء الحكومات والوزرات وتقييمها، بل وطرح الثقة فيها، فتظهر لدينا ديمقراطية جديدة هي ديمقراطية البلوك تشين.

وقد تطرح تقنية البلوك تشين الإشكالية التي أثارتها شبكات التواصل الاجتماعي أثناء الثورات العربية، من حيث الدور التعبوي الذي قامت به،

وتسبب في زيادة أعداد المظاهرات في مختلف الدول العربية، فالأمر قد يتكرر مرَّة أخرى مع تقنية البلوك تشين، ولكن بصورة قد تكون أقوى من ذي قبل، وذلك لأن جميع الأفراد الموجودين بالسلسلة هم أفراد فعليون، وليس الأمر مجرد رأي عام إلكتروني يمكن تزويره عبر برامج وتطبيقات خبيثة كما هو الحال في مواقع التواصل الاجتماعي، وبالتالي قد تكون ذات مصداقية أكثر وخطورة أكبر من الشبكات الاجتماعية.

ومن ناحية أخرى، سوف تُحدث البلوك تشين ثورة كبيرة في عالم الإدارة قد تساهم في القضاء على الفساد، بما يحقق الكفاءة والفاعلية السياسية والإدارية أيضًا، فمن ناحية يساعد هذا النظام الدوائر الحكومية على تحقيق الفاعلية، فجميع المعاملات الخاصة بالأفراد يمكن أن تكون واضحة داخل السلسلة، وإذا كان هناك حاجة للتأكد من بعض المعلومات أو الشهادات أو الوثائق يمكن بسهولة الاطلاع عليها، ما يساعد في توفير الوقت والقضاء على الروتين[1].

كما يساعد ذلك في تتبع جميع الخطوات الخاصة بالمعاملة، وذلك لأن نظام البلوك تشين لا يسمح بالتعديل أو الإلغاء، فجميع المعاملات التي تتم عليه مسجلة خطوة بخطوة بالتوقيت، وفي حالة التلاعب أو التزوير لا تقبل السلسلة إدخال المعاملة مرَّة أخرى، بما يساعد في القضاء على الفساد الإداري والمالي وتحسين توجيه النفقات المالية؛ وهو ما ينعكس في النهاية على النظام السياسي بصورة إيجابية، حيث تتحسن صورته الذهنية لدى الشعب، ما يزيد من فرص الاستقرار السياسي.

من جانب آخر، تساهم البلوك تشين في تسهيل الإجراءات الحكومية والروتينية الخاصة بالأفراد، وذلك عبر التخلص التام من استخدام الوثائق

1- Sean Williams, 5 Big Advantages of Blockchain, and 1 Reason to Be Very Worried, Fool, Dec 11, 2017, accessed Feb 15, 2018 on: https://bit.ly/2RFc24Q

الورقية واستبدالها بالسجلات الرقمية والوثائق الموقعة رقميًّا، والتخلص من العمليات اليدوية من خلال الجمع بين الأطراف ذات الصلة الذين يشاركون في العملية نفسها؛ ولذلك يمكن لجميع المتعاملين إنهاء أي معاملة إدارية دون الحاجة إلى الوجود داخل المؤسسة، ويشمل ذلك الموظف والعميل، ومن ثم سرعة إنهاء المعاملات دون الحاجة إلى التقيد بمكان جغرافي، بما يحقق في النهاية «سعادة» المتعاملين، فتنتقل الدول من مرحلة تقديم الخدمة إلى مرحلة إسعاد المتعاملين.

ب- التداعيات الاجتماعية:

يُعتبر التهديد الأكبر لتقنية البلوك تشين اجتماعيًّا بالأساس، وذلك بسبب التحديات التي يطرحها أمام كثير من المؤسسات الحكومية وغير الحكومية، وبصورة خاصة في قطاعات المال والإدارة والأعمال الوسيطة، والتي أضحت وظائفها مهددة، بل إن الأمر قد يتجاوز هؤلاء إلى الشركات العالمية التي تعمل في مجال الوساطة، مثل «أمازون»، و«علي بابا» التي تقوم بدور الوسيط بين البائع والمشتري، وكذلك «إير بي إن بي» Airbnb عملاق السمسرة العقارية التي تقوم بدور الوسيط بين المؤجر والمستأجر، وكذلك الشركات التي تعمل في قطاع النقل الأجرة مثل «أوبر»، و«كريم»، وغيرهما، فجميع هذه الشركات أيضًا مهددة من تقنية البلوك تشين، حيث سيصبح التواصل بين البائع والمشتري يتم بصورة مباشرة عبر النظام الآمن لسلسلة الكُتلة.

وهناك تحديات اجتماعية أخرى تطرحها البلوك تشين غير التوظيف، حيث يمكن استخدامها في أعمال غير قانونية، مثل تجارة المخدرات والبغاء والسلع الممنوعة والأسلحة، ما يهدد السلم المُجتمعي ويضر بمصالح الأفراد، فضلًا عن إمكانية التعرف على بعض المعلومات الشخصية الخاصة بالأفراد الموجودين في السلسلة وتهديدهم، ومن ذلك مثلًا معرفة أن أحد الأشخاص

بصدد الحصول على تحويل مالي كبير عبر البلوك تشين، ما قد يجعله هدفًا لبعض العصابات التي تراقب بياناته على نفس سلسلة الكُتلة.

رابعًا: العُملات الافتراضية

انتشرت في السنوات الأخيرة النقود الرقمية أو العُملات الافتراضية، ووصل عددها إلى ما يقرب من 2000 عملة حول العالم مع بداية عام [1]2018، وليست جميعها بالطبع لها رواج، بل أشهرها رواجًا عملة البيتكوين. وعلى الرغم من أن العُملات الرقمية لا تتوفر لها حتى الآن الشروط والمعايير التي استقرت بالنسبة للعُملات النقدية التقليدية، ولا يوجد لها إطار قانوني واضح يحكم تعاملاتها، فإن هناك أكثر من 3 ملايين مستخدم نشط حول العالم يستخدمونها في تعاملاتهم اليومية[2].

1- خصائص العُملات الافتراضية:

على الرغم من هذا الانتشار، فإن هناك خلطًا بين الرقمي والافتراضي، فالعُملات الافتراضية هي تلك العُملات المتاحة فقط في شكل رقمي دون أن يكون لها أصل مادي ملموس، أي تلك العُملات التي تتكون من أصفار وآحاد تمثل البنية الأساسية للعالم الرقمي، على عكس النقود الرقمية الحقيقية التي يقصد بها «النقود التقليدية التي يتم تداولها عبر الحسابات البنكية والمحفظة في شكل أرقام على أجهزة الكمبيوتر، تتم تسويتها في النهاية بالعُملات التقليدية»؛ ولذلك فإن كل النقود الافتراضية هي نقود رقمية، ولكن العكس ليس صحيحًا[3].

وتتميز العُملات الافتراضية بعدة خصائص، فمثلًا لا تخضع لأي إطار قانوني واضح، ولا تصدر عن أي من البنوك المركزية، ولا تخضع بالتالي لسيطرة

1- All Cryptocurrencies, Coinmarketcap, Nov, 11, 2017, on: https://coinmarketcap.com/all/views/all/

2-Garrick Hileman & Michel Rauchs, GLOBAL CRYPTOCURRENCY BENCHMARKING STUDY, Cambridge Centre for Alternative Finance,

3- Andrew Wagner, Digital vs. Virtual Currencies, Bitcoin Magazine, Issue 22, Aug 22, 2014, accessed December 17, 2017 on: https://bitcoinmagazine.com/articles/digital-vs-virtual-currencies-1408735507/

الدولة بأي شكل، ولذا يختلف المحللون حول تقييم العُملات الافتراضية وفقًا للمعايير الوظيفية للعملة، وهي أنها وسيط للتبادل ووحدة للحساب ومخزن للقيمة، كما أن نظام العُملات الافتراضية القائم على البلوك شين أو سلسلة الكُتلة يُعد نقيضًا لأنظمة البنوك المركزية التي تتدخل بسياساتها للتأثير على مستويات العرض والطلب للعُملات؛ مما يؤدى أحيانًا إلى التضخم وانخفاض القوة الشرائية للعملة.

وتختلف نوعيَّة التعاملات بالعُملات الافتراضية، فبينما يستخدمها عديد من الأفراد والشركات في معاملات تجارية مشروعة، فثمة تعاملات أخرى غير مشروعة تتم عبر ما يعرف باسم «الشبكات الداكنة Dark Net، التي يتم فيها الاتجار بالمخدرات، والأسلحة، أو تمويل تنظيمات إرهابية[1].

2- آلية عمل العُملات الافتراضية:

يُعتبر نظام سلسلة الكُتلة بمثابة «الجسر الرقمي المشفر» الذي يضمن انتقال المعاملة – أي معاملة - من الطرف (أ) إلى الطرف (ب) بكفاءة وفاعلية، ويربط جميع المعاملات والتحويلات بعضها ببعض لضمان إحكام السيطرة عليها في مكان واحد وآمن، ولذلك فهي الآلية الرئيسية التي تعمل بها العُملات الافتراضية على سبيل المثال مثل البيتكوين[2].

ويستطيع كل مستخدم حول العالم الدخول إلى نظام سلسلة الكُتلة الخاصة بالمعاملة التي يرغب في القيام بها، فمثلًا إذا كان الغرض نقل عملة إلكترونية،

1- Andolfatto, David. 2014. Bitcoin and Beyond: The Possibilities and Pitfalls of Virtual Currencies. Federal Reserve Bank of St. Louis, March 31, 2014, accessible at: http://www.stlouisfed.org/dialogue-with-the-fed/assets/Bitcoin-3-31-14.pdf
2- Ed Clowes, Staff Reporter, What is blockchain, and why do the UAE and Saudi Arabia want to use it?, Gulfnews, December 16, 2017, accessed December 17, 2017, on: http://m.gulfnews.com/business/sectors/technology/what-is-blockchain-and-why-do-the-uae-and-saudi-arabia-want-to-use-it-1.2141837

سيقوم المستخدم بإنشاء محفظته الخاصة، التي سيتم إرسال النقود منها وإليها، ثم تحديد المبلغ المرجو تحويله عبر نظام سلسة الكُتلة إلى الطرف الآخر، والذي قد يكون شركة، أو شخصًا، أو خلافه، وبمجرد إرسال المعاملة يقوم ملايين من المنقبين حول العالم الذين يجلسون خلف أجهزتهم بإجراء مجموعة من العمليات الحسابية المعقدة عبر أجهزتهم بغرض التأكد من صحة المعاملة، وبمجرد أن يتم التأكد منها حتى يسمح لها بالدخول في السلسة، وتضم إلى غيرها من الكتل مكونة في النهاية سلسلة الكُتلة؛ مما يعني اشتراك ملايين من الأجهزة حول العالم في التأكد من صحة المعاملة قبل إتمامها، وهو ما يجعل عملية اختراق النظام أو التلاعب به أمرًا صعبًا للغاية لأنه يتطلب اختراق جميع هذه الأجهزة في الوقت نفسه.

ويحصل هؤلاء المنقبون على مكافآت مالية نظير عملية التدقيق الحسابي التي قاموا بها؛ فإذا كان الأمر نقل عملة البيتكوين، فإنهم يحصلون على نسبة من عملية التنقيب ضئيلة جدًّا، ولكنها موزعة على جميع من شاركوا في العملية، مما يحقق مبدأ المساواة في توزيع الثروة على الرغم من ضآلة هذه الثروة، وبالتالي تمكن هذه التقنية أي جهتين من تبادل أي أموال ذهابًا وإيابًا دون الحاجة إلى وسيط مالي بالاعتماد على وسائط تقنية تستخدم سلسلة الكتل، مثل Due.com، مما يعني التخلص من الرسوم الهائلة وتسريع عملية تحويل الأموال من 3-7 أيام إلى بضع دقائق مقابل رسوم رمزية تمثل رسوم استخدام النظام، وليس رسوم وساطة.

خامسًا: الطابعات ثُلاثيَّة الأبعاد

أضحى استخدام الطابعات ثُلاثيَّة الأبعاد في مختلف المجالات أمرًا واقعًا لا مفرَّ منه، سواءً في صناعة النقل، كالسيارات، والسفن، والطائرات، أو في مجال الفضاء كالمركبات الفضائية، والصواريخ، أو في صناعة الأسلحة كالمسدسات، والبنادق، والمعدات الثقيلة، أو في مجال الطب، كصناعة الأعضاء البشرية، والألياف، أو في مجال البناء والتشييد، وإنشاء البيوت والمكاتب، أو حتى في مجال الصيدلة كتصنيع الأدوية ومستحضرات التجميل، وغيرها من الصناعات.

وعلى الرغم من الأهمية المتزايدة لتوظيف الطابعات ثُلاثيَّة الأبعاد في مختلف الصناعات والمجالات، بما يوفر الوقت والجهد ويزيد من كفاءة وسرعة عملية الإنتاج، فإنه يمكن استخدامها أيضًا فيما يمكن اعتباره تهديدًا للأمن المُجتمعي، بل والأمن القومي للدولة، وذلك من خلال استخدامها في تصنيع الأسلحة من قبل أفراد عاديين، أو من قبل جماعات إرهابية، أو استخدامها في عمليات تقليد المنتجات بما ينتهك حقوق الملكية الفكرية التي تنص عليها المواثيق الدولية، أو في تزوير التماثيل والتحف التاريخية، أو في صناعة المخدرات، فضلًا عما تثيره طباعة الأعضاء البشرية من إشكاليات أخلاقية.

شهد سوق الطابعات ثلاثية الأبعاد في العالم نموًا مركبًا في آخر خمس سنوات، فقد ازداد من بيع 106.761 وحدة في عام 2014، إلى 490 ألف وحدة في عام 2016، ويتوقع أن يتضاعف هذا الرقم سنوياً حتى عام 2020، وحينها سوف يصل الرقم تقريباً إلى 5.6 مليون وحدة. وينطبق هذا الأمر على منطقة الشرق الأوسط التي نما فيها السوق بنسبة بلغت 59% في عام 2017.

وتتزايد خطورة استخدام هذا النوع من الطابعات مع توافرها للاستخدام التجاري للأفراد، حيث كشفت شركة HP عن خطتها لتقديم طابعات ثُلاثيَّة

الأبعاد للاستخدام المنزلي، وأشارت الدراسة التي قامت بها مؤسسة «IDC» المتخصصة في مجال أبحاث السوق، إلى أن سوق الطابعات الثلاثية في منطقة الشرق الأوسط ينمو بمعدل مركب سنوي وصل إلى 59% في عام 2017 من حيث عدد الطابعات التي تصل إلى أسواق المنطقة، وبنسبة 29% من حيث عوائد استثماراتها.

كما بلغ عدد الطابعات ثُلاثيَّة الأبعاد التي تم بيعها على مستوى العالم خلال عام 2014 نحو 106 آلاف و761 وحدة، وارتفع هذا الرقم في عام 2015 إلى 244 ألفًا و533 وحدة، وبلغ في نهاية عام 2016 نحو 490 ألف وحدة. ويُتوقع أيضًا أن ترتفع مبيعات هذه الطابعات لما يزيد على الضعف سنويًّا خلال الفترة بين أعوام 2017 و2020، وبحلول ذلك الوقت من المتوقع أن تصل شحنات مبيعاتها العالمية لأكثر من 5.6 مليون وحدة.

ولا تزال دول أمريكا الشمالية وغرب أوروبا تهيمن على مبيعات الطابعات ثُلاثيَّة الأبعاد بنسبة 66.2%، ولكنها بدأت بالتراجع نسبيًّا لصالح الصين، التي باتت تحقق أعلى معدل نمو سنوي في الطابعات ثُلاثيَّة الأبعاد بنسبة بلغت 172.9%، وذلك بالاعتماد على دعم وطني للتقنية وللاستثمارات بمجالات التعليم والنشاط التجاري والبحث[1].

ولمَّا كانت تقنية الطابعات ثُلاثيَّة الأبعاد حديثة نسبيًّا، فضلًا عما تشهده من تطورات مستمرة من حيث الأنواع وطرق الطباعة والمواد المستخدمة في هذه العملية، فإن التشريعات والقوانين المنظمة لاستخدام هذا النوع من الطابعات ما زالت تعاني قصورًا شديدًا، كما أن الجدل لا يزال مستمرًا في عديد من الدول، مثل الولايات المتحدة الأمريكية، وإنجلترا، ودول الاتحاد الأوروبي، حول عملية

1- الطابعات ثُلاثية الأبعاد... مستقبل واعد»، صحيفة الشرق الأوسط، 20 أكتوبر 2015، متاح على الرابط التالي: http://bit.ly/1ZJtBuX.

التقنين، نظرًا لقصر الخبرة التاريخية في استخدام هذه التقنية وحداثتها النسبية وقلة عدد الحالات التي شكلت خطورة في استخدامها، بل إن محاولات التقنين التي تمت قد جاءت تجارية إلى حد كبير ممثلة في أجهزة، مثل إدارة الأطعمة والعقاقير الطبية الأمريكية، بهدف ضمان جودة المنتجات المُصنَّعة من خلالها، والحفاظ على صحة وحياة المستهلك النهائي، وليس بهدف تجنب التهديدات الأمنية الناجمة عنها.

وقد يرجع ذلك إلى أن الطابعة ثُلاثيَّة الأبعاد هي مجرد آلة في النهاية تُستخدم في عملية الإنتاج، والقانون التقليدي ينظم هذه العملية، حيث يضع قيودًا صارمة على استخدامها فيما يهدد أمن وسلامة المواطنين والمُجتمع، فمثلًا يحظر القانون صناعة المخدرات، بغض النظر عن الوسيلة التي تم استخدامها في تحضيرها، كما يحظر أيضًا صناعة الأسلحة لغير الجهات المرخص لها، لكنه من الضروري إعادة النظر فيما يتعلق بالمواد المستخدمة في عملية الطباعة، حيث يمكن صناعة مسدس مثلًا من البلاستيك يستخدم في ترويع المواطنين.

1- تطبيقات الطابعات ثُلاثيَّة الأبعاد:

تتعدد وظائف استخدام الطابعات ثُلاثيَّة الأبعاد، في جميع المجالات، سواءً في التصنيع بصفة عامة، أو في مجال البناء، والطب، والنقل، والفضاء، وصناعة الأسلحة والأطعمة ومستحضرات التجميل، وغيرها من مئات المجالات التي دخلت بالفعل في إنتاجها.

وفيما يلي عرض بأهم مجالات استخدامها وفق التجارب الدولية، وهي:

أ- في مجال البناء:

قامت شركة صينية ببناء 10 منازل، كاملة الحجم، مُكوَّنة من طابق واحد، باستخدام تقنية الطباعة ثُلاثيَّة الأبعاد، خلال يوم واحد. وقد استعانت الشركة

في إنجاز هذه المنازل بأربع طابعات ثُلاثيَّة الأبعاد، بمقاسات 10*6.6 أمتار، مستخدمة خليطًا من الإسمنت ومخلفات البناء المُعاد تدويرها لبناء الجدران.

وقد تميزت برخص تكلفتها، إذ إن تكلفة البناء لم تتجاوز 5 آلاف دولار، لكل وحدة، طبقة بعد طبقة، إلى أن يتم تكوين المنزل[1]، وقبل هذا الاكتشاف الصيني تم بناء منزل من خمسة طوابق في أمستردام عن طريق الطوب المطبوع مع البلاستيك المعالج[2]، ليس هذا فحسب، بل يقدم موقع http://www.wiki-house.cc خدمة تصميم وبناء منزل من خلال الطباعة ثُلاثيَّة الأبعاد. كما أعلنت حكومة دبي عن إنشاء أول مكتب في العالم مصنوع بالكامل من خلال الطابعة ثُلاثيَّة الأبعاد في مايو 2016.

ب- في مجال النقل:

بدأت شركات النقل، خاصة في مجال صناعة الطائرات، في الأخذ بتقنية الطباعة ثُلاثيَّة الأبعاد في وقت مبكر من ظهورها في تطوير وصناعة النماذج الأولية، وهناك عديد من شركات صناعة الطيران التي تعتمد الآن على تلك التقنية مثل: «إيرباص»، و»جي آي»، و»بوينج»، إلا أن الطبيعة الحرجة لصناعة الطيران تجعل استخدام تلك التقنية في تلك الأوقات مقتصرًا على قطع الغيار غير الحساسة في الطائرات.

ولم يختلف الأمر في صناعة السيارات، حيث اتجه المصنعون لاستخدام تلك التقنية في وقت مبكر، خاصة الشركات المعنية بالسيارات الرياضية. وتُستخدم تلك التقنية في مجال صناعة السيارات بصورة بارزة في عملية صناعة قطع

1- الصين: بناء 10 منازل في يوم واحد عبر «طابعات ثلاثية الأبعاد»، جريدة الحياة، 27 أبريل 201. http://goo.gl/9s2H4P

2- تطوير طابعة ثلاثية الأبعاد للمساعدة في بناء منازل صغيرة بالصين، شبكة محيط، 28 سبتمبر 2014.: http://goo.gl/tFoIGE

الغيار، خاصة مرحلة ما بعد البيع، وذلك نظرًا لسرعة إنتاجها حال الطلب[1]، حيث أقامت شركة «Local Motors» الأمريكية في أبريل 2014 مسابقة لاختيار أفضل تصميم سيارة تمت طباعتها من خلال 3D Printer، وقد فازت فيها السيارة «Starti» بجائزة قدرها 5 آلاف دولار، من بين 200 متسابق، وبرزت ستة تصاميم أخرى في المسابقة ليفوز كل منها بألف دولار أمريكي، وقد تطلب طباعة النموذج الأول للسيارة الفائزة«Starti» 40 ساعة، أما عملية التجميع فاستغرقت أربعة أيام فقط[2].

ولم تكن هذه هي أولى المحاولات، فقد سبقها قيام مجموعة من المصممين الأمريكيين بتقديم أول سيارة في العالم مصنوعة بطابعات الـ3D كسيارة تجريبية، وقد أطلق المصممون على هذه السيارة التي يبلغ وزنها 545 كيلو جرامًا فقط اسم أوروبي «Urbee»، والتي تم تصميمها بثلاثة إطارات فقط، ومنحوها محرِّكًا هجينًا يعمل بوقود الإيثانول والكهرباء، ويعتبر هذا المحرك - بالإضافة إلى الشاسيه - المكونات الوحيدة المصنوعة من المعدن في هذه السيارة، حيث تصل قوة محرك هذه السيارة إلى 10 أحصنة، ويمكن أن تتخطى سرعتها القصوى أكثر من 64 كم/ساعة في حالة استخدام محرِّك الإيثانول[3]. وقد أدخلت شركة «فورد» الأمريكية هذه الطباعة إلى صناعة السيارات لإنتاج الأجزاء النموذجية للسيارة بسرعة فائقة، مثل رؤوس الأسطوانات، ومشعب السحب، وفتحات الهواء.

ج-في مجال الطب:

شاع استخدام الطباعة ثُلاثيَّة الأبعاد في أكثر من منحى بالمجال الطبي، بداية

1- the free beginner’s guide to 3d printing, Op.cit, ch 8, p60-63.

2- سيارات المستقبل.. هل ستصنع بالطباع ةثلاثية الأبعاد؟، موقع سي إن إن، 26 يونيو 2014، للمطالعة:
http://arabic.cnn.com/scitech/2014/06/26/gallery-futurisitc-drive-step-inside-3d

3- تعرف على Urbeeأول سيارة في العالم مصممة بطابعات 3D، مارس 2014،
http://www.akhbarak.net/news/2014/02/22/4039383#

من عملية التشخيص للأمراض الأكثر تعقيدًا وصعوبة على الأشعَّة التلفزيونية والرنين والموجات الصوتية، مثل السرطان، وغيره من الأمراض المُستعصية، وكذلك في علم الأجنَّة من حيث الكشف عن التشوُّهات في مراحل مبكرة من عُمر الجنين. كما تمكنت بعض التجارب من استخدام تلك التقنية في صناعة الأطراف الصِّناعيَّة والأجهزة التعويضية بتكلفة أقل من تلك التي تنتج بالطرق التقليدية، إلى جانب هذا دخلت الطباعة ثُلاثيَّة الأبعاد في صناعة المعدات الطبية وأدوات الجراحة، وصناعة نماذج مماثلة للجسم البشري للتعلم والدراسة عليها، وكذلك طباعة الشرايين والأوعية الدموية[1]

وقد توصل باحثون صينيون إلى ابتكار طابعة ثُلاثيَّة الأبعاد قادرة على صنع الأعضاء البشرية من الخلايا، ويعتمد هذا النوع من الطابعة البيولوجية التي أطلق عليها اسم «ريجينوفو»، على نوع من الهايدروجيل الذي يشبه الجيلاتين، أو الكولاجين، ويملك خصائص فيزيائية تشبه الأعضاء البشرية. كما توصل فريق من الباحثين الصينيين في جامعة «هانغزو للعلوم والتكنولوجيا» إلى صنع كلية ثُلاثيَّة الأبعاد، لكنها تفتقر إلى الأعصاب والأوعية الدموية في الوقت الحالي، ويصبح التحدي الأكبر هو العثور على طريقة ما لهندسة الأعضاء المطبوعة بحيث يقبلها الجسم[2].

ولا يُعَدُّ هذا الابتكار الصيني الأول من نوعه، فالباحثون في الولايات المتحدة متقدمون في هذا المجال، ففي عام 2013، حصل طفل يبلغ عامين من العمر على قصبة هوائية صنعت من الخلايا الجذعية الخاصة به[3]. وفي برلين، استخدمت التقنية نفسها لإنتاج صمام قلب بشري مماثل تمامًا لقلب المريض،

1C. Lee Ventola, Medical Applications for 3D Printing: Current and Projected Uses, NCBI, url: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4189697/

2- طابعة ثلاثية الأبعاد للأعضاء البشرية، موقع سكاي نيوز عربي، 11 نوفمبر، 2013.
http://goo.gl/Sl6dK6

3- الطباعة الثلاثية الأبعاد للأنسجة والأعضاء البشرية ستثير جدلًا أخلاقيًا، موقع إيلاف، 1 فبراير 2014. http://www.elaph.com/Web/LifeStyle/2014/2/872934.html

حيث يتم في البداية تصوير مقطعي لصمامات قلب المريض، وبعدها يأتي دور الطابعة ثُلاثيَّة الأبعاد، فيتم إرسال هذه البيانات الهندسية إليها، ثم تتولى هي إنتاج صمامات قلب بلاستيكية.

ويسعى الباحثون الآن إلى الانتقال بهذه الخطوة إلى الخلايا البشرية عن طريق الاستعانة بأنسجة «الحبل السري» الذي يحتوي على الخلايا الجذعية. وتقوم أبحاث علمية لتطوير صمامات قلب اصطناعية تنمو فيها الخلايا، وبعد أن تنمو تُزرع في جسم المريض لتقوم بالوظيفة الكاملة التي يقوم بها صمام القلب البشري[1].

د- في مجال صناعة الأسلحة:

قامت شركة «سوليد كونسيبتس»، ومقرها في كاليفورنيا، بصنع أول مسدس فولاذي، بفضل طابعة ثُلاثيَّة الأبعاد، والسلاح مؤلف من أكثر من 30 قطعة، وبعضها كان من الفولاذ غير القابل للصدأ، وأكدت الشركة أن المسدس «يعمل بشكل جيد»، موضحة أنها أطلقت نحو 50 طلقة أصابت وسط هدف يبعد أكثر من 25 مترًا[2]، ولعل الأمر ليس بالجديد، ولكن الجديد فيه هو صناعة المسدس من الفولاذ، فقد أُلْقِيَ القبض على رجل ياباني يبلغ من العمر 27 عامًا؛ لامتلاكه أسلحة ومسدسات مطبوعة بالتقنية ثُلاثيَّة الأبعاد[3].

وتمكنت شركة "ديفينس ديستربيوتد" في مايو 2013 من صناعة أول مسدس بتكنولوجيا الطباعة ثُلاثيَّة الأبعاد في الولايات المتحدة، وسمَّته "ليبِرايتور Liberator"، وتمت تجربته عمليًّا بنجاح تام[4].

1-http://al-akhbar.com/node/211143

2-تصنيع أول سلاح فولاذي بفضل طابعة ثلاثية الأبعاد، موقع العربية، 9 نوفمبر 2013، للمطالعة: ttp://goo.gl/xwUjyf.

3- القبض على ياباني صنع مسدسات باستخدام طابعة ثلاثية الأبعاد، موقع عالم التقنية، 9 مايو 2014. http://goo.gl/zrPYTG/

4- كرم سعيد «الطباعة ثلاثية الأبعاد: ثورة صناعية للقرن 21»، موقع صحيفة الحياة، 1 سبتمبر 2015، متاح على الرابط التالي: http://bit.ly/1Udc24N.

وفي أفغانستان، يستخدم الجيش الأمريكي عدة طابعات ثُلاثيَّة الأبعاد لإنتاج قطع تبديل التجهيزات العسكرية في الميدان عند الحاجة، وبسرعة فائقة، دون الحاجة إلى طلب هذه القطع من واشنطن وانتظار وصولها[1].

ولا يقتصر الأمر على الأسلحة الخفيفة فقط، بل يمتد إلى الأسلحة الثقيلة أيضًا، فقد حلَّقت مقاتلات بريطانية للمرَّة الأولى بقطع غيار صُنعت بتكنولوجيا الطباعة ثُلاثيَّة الأبعاد، وأعلنت شركة BAE Systems للصناعات العسكرية، أن قطع الغيار المعدنية استُخدمت بنجاح في مقاتلات تورنايدو، أقلعت من مطار الشركة في وارتن بمقاطعة لانكشير شمال غربي إنجلترا[2].

هـ- في مجال الفضاء:

تدخل تقنية الطباعة ثُلاثيَّة الأبعاد في الصناعات المتعلقة بالفضاء، حيث تمكنت وكالة ناسا من استخدام تلك التقنية في تصنيع أجزاءٍ من المركبات الفضائية، وكذلك في مكونات مُحرِّكات الصواريخ، حيث قامت الوكالة في نوفمبر 2014 بإنتاج أول قطعة تسمى "An Extruder Plate"، أو الطبق الطارد، كخطوة مبدئية لتصنيع قطع من المركبات خارج الكرة الأرضية في السنوات المقبلة، وطبقًا للدراسات التى أُجرِيَت داخل الوكالة، فإن نحو 30% من أجزاء المركبات يمكن صناعتها بواسطة طابعة ثُلاثيَّة الأبعاد[3].

وفي وكالة ناسا للفضاء، أطلقت شركة SpaceX أجزاءً لصاروخ تمت صناعته بتقنية الطباعة ثُلاثيَّة الأبعاد، كما تستخدم الشركة على استخدام تلك التقنية أيضًا في تصنيع صواريخ هروب طوارئ للمركبة الفضائية التابعة لها دراجون

1- محمد أنس طويلة «مستقبل الطباعة ثلاثية الأبعاد»، موقع الجزيرة نت، 25 سبتمبر 2013، متاح على الرابط التالي: http://bit.ly/28vJRpn.

2- مقاتلات بريطانية تُحلِّق للمرَّة الأولى بقطع غيار صنعتها طابعة ثلاثية الأبعاد، موقع إيلاف، 7 يناير 2014، للمطالعة: http://www.elaph.com/Web/news/2014/1/864776.html#sthash.reRyxLk4.dpuf

3-Mike Wall. How 3D Printing Could Aid Space Exploration, space.com, url: http://www.space.com/27860-3d-printing-space-exploration.html

Dragon، وتحاول وكالة الفضاء الأوربية "ESA" تطوير طابعة ثُلاثيَّة الأبعاد تستخدم موادَّ قمريَّة لبناء قاعدة قمريَّة.

كما نجح فرع "شانغهاي البحثي" للشركة الصينية لعلوم وتكنولوجيا الفضاء، في صناعة آلة للطباعة ثُلاثيَّة الأبعاد يمكن لرواد الفضاء استخدامها عند قيامهم بمهام فضائية، وهي قادرة على طباعة دعائم العدسات البصرية المستخدمة في معدات فضائية، ومكونات معقدة تستخدم في معدات اختبار الطاقة النووية، وضواغط تستخدم في بحوث الطائرات، وتروس ذات أشكال خاصة تستخدم في مُحرِّكات السيارات[1].

و- في مجال صناعة الأطعمة:

يُعَدُّ استخدام تقنية الطابعات ثُلاثيَّة الأبعاد في مجال الأطعمة من الاستخدامات الحديثة، حيث عملت شركات الأطعمة العاملة في ذلك المجال على توظيفها في عملية إعداد وتقديم الطعام، وبدأت تلك التقنية في صناعة الحلويات، مثل الشوكولاتة، ثم تطورت واستخدمت في طباعة اللحوم على البروتينات الخلوية.

وقد كشفت شركة "ناتشرال ماشين" عن طابعة "فوديني" Foodini التي يظهر من اسمها أن مهمتها إنتاج الأطعمة، وقد بلغ تكلفة طابعة "فوديني" قرابة 1300 دولار، وتتميز بصغر حجمها الذي يماثل كثيرًا الميكروويف. كما أعلنت وكالة الفضاء الأمريكية "ناسا" أن رواد الفضاء في المستقبل سوف يحملون معهم إلى الفضاء طابعات ثُلاثيَّة الأبعاد لمساعدة رواد الفضاء على صناعة المعدات، بل والأطعمة التي يحتاجون إليها أثناء رحلاتهم الفضائية، حيث أعلنت شركة أمريكية تحمل اسم "ميد إن سبيس"، أي "صُنع في الفضاء"، أنها تختبر طابعات ثُلاثيَّة الأبعاد في مناطق انعدام الجاذبية لصالح وكالة ناسا،

1- «الصين تصنع طابعة ثلاثية الأبعاد يمكن استخدامها في الفضاء»، موقع الحرة، 8 ديسمبر 2014، متاح على الرابط التالي: http://www.alhurra.com/content/First-three-d-space-based-printer/262857.html.

وأوضحت أن الاختبارات تتركز على معرفة الآثار طويلة المدى لانعدام الجاذبية على هذه التقنية[1].

ي- استخدامات أخرى متنوعة:

هناك مئات من الاستخدامات الأخرى للطبعات ثُلاثيَّة الأبعاد، بالإضافة إلى ما ذكر أعلاه؛ إذ يمكن طباعة مساحيق التجميل، مثل أحمر الشفاه، حيث يتم فقط اختيار اللون المفضل، ثم تتولى الطابعة تقديم المنتج. كما تكمنت مؤسسة Smithsonian من الحفاظ على التماثيل التاريخية النادرة، فبدأت برقمنة كثير من التماثيل النادرة، للبدء بطباعتها مرَّة أخرى، وتوفير نسخ كثيرة منها.

من ناحية أخرى، تدخل تقنية الطباعة ثُلاثيَّة الأبعاد في عملية صناعة المجوهرات بجميع مراحلها، بدءًا من صناعة قوالب الصب والطلاء والنقش، وصولًا إلى الإنتاج النهائي لها، ويعتمد الفاعلون في ذلك المجال على عديد من البرمجيات التي من شأنها تطوير عملية الصناعة، مثل 3D Cad.

2- التهديدات الأمنية للطابعات ثُلاثيَّة الأبعاد:

على الرغم من وجود عديد من الإيجابيات للطباعة ثُلاثيَّة الأبعاد، فإن هناك عديدًا من التهديدات والاستخدامات السلبية لتلك التقنية، يمكن تناولها فيما يلي:

أ- استخدامها في صناعة الأسلحة:

تُمكِّن الطباعة ثُلاثيَّة الأبعاد أي شخص من صناعة سلاح في بضع دقائق بمنزله، ولعل مثال "كودي ويلسون" طالب القانون بولاية تكساس الأمريكية البالغ من العمر 24 عامًا، والذي قام في مايو 2013 بصناعة مسدس من البلاستيك

1- ناسا توضح استخدامات الطباعة ثلاثية الأبعاد في الفضاء، موقع عربي!، 3 يونيو 2013، للمطالعة: http://www.arabia.com/women/details/19016

باستخدام تقنية الطباعة ثُلاثيَّة الأبعاد أطلق عليه The Liberator.8 خير مثال على ذلك، وبعدما قام بتصنيع السلاح نشر على الإنترنت تصميم CAD يشرح طريقة إنتاج السلاح، وتم تحميل هذا الملف 100000 مرَّة في يوم واحد، حتى أشارت وزارة الخارجية الأمريكية إلى أن هذا الملف ستتم إزالته من الإنترنت.

وما يجعل من هذا الأمر تهديدًا مباشرًا هو أن المعدات الأمنية المستخدمة للكشف عن الأسلحة لا يمكنها كشف هذا النوع من الأسلحة المصنوعة من البلاستيك، فضلًا عن إمكانية صناعتها من خلال المواد الصلبة كما فعلت شركة "سوليد كونسيبتس"، كما أن تلك الأسلحة لا تملك أرقامًا مسلسلة، مما يسهل استخدامها دون التعرف على مستخدميها[1].

لا تمنع الفوائد الكثيرة لاستخدام الطابعات ثلاثية الأبعاد من التأكيد على أن عدم تقنينها وفق تشريعات وقوانين تنظم استخدامها وتداولها سوف يزيد من تداعياتها السلبية على الأمن الوطني والمجتمعي، إذ يمكن توظيفها في تصنيع الأسلحة من قبل أفراد عاديين أو من قبل جماعات إرهابية، وفي عملية تقليد المنتجات بما ينتهك حقوق الملكية الفكرية، وكذلك يمكن استخدامها في صناعة المخدرات وتزوير التحف الفنية والآثار التاريخية، بل وفي طباعة الأعضاء البشرية، بما يثيره ذلك من قضايا أخلاقية.

ب- الاستخدامات الإرهابية:

إن أحد أهم العيوب المترتبة على استخدام تلك التقنية في صناعة الأسلحة، أنها تعد إحدى الوسائل المساعدة للتنظيمات الإرهابية والإرهابيين، من حيث سهولة توفير الأسلحة وتصنيعها في أوقات قليلة، وطبقًا لتصريحات "مارك رولي"، رئيس شرطة لندن والمفوض المساعد، فإنه يمكن للإرهابيين استخدام تلك التقنية في طباعة "طائرات من دون طيار"–على غرار تلك المطبوعة بواسطة مشروع diy- أو في صناعة

1- Craig Schwartz, 3-D Printing: The Potential Implications and Challenges for Law Enforcement, policechiefmagazine, url:http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=3662&issue_id=32015

القنابل أو بنادق ورصاص، ولأن المواد المستخدمة في تلك الأجهزة من الصعب اكتشافها بواسطة الأجهزة الأمنية، فإن ذلك يُعَدُّ مهددًا كبيرًا وتطوُّرًا ملحوظًا في النشاط الإرهابي[1].

ج- احتمالية استخدامها في إنتاج المخدرات:

إذا كانت أحد أهم الجوانب الإيجابية للطباعة ثُلاثيَّة الأبعاد هو استخدامها في المستقبل في صناعة الأدوية بالمنازل عن طريق توفر ملف الطباعة على الإنترنت وحقن تلك الآلات بالمواد الكيميائية اللازمة لصناعة الأدوية، فإن هناك عديدًا من التقارير التي تشير إلى احتمالية استخدام ذلك بصورة سلبية[2]؛ فوفقًا للبروفسير "لي كرودين" وفريقه البحثي المكون من 45 باحثًا بجامعة جلاسكو في أسكتلندا، فإنه يمكن استخدام مواد كيميائية في الطباعات ثُلاثيَّة الأبعاد لصناعة المواد المخدرة، خاصة مع توفر بعض المواد مثل البارافين والزيوت النباتية التي تدخل في صناعة تلك المواد[3].

د- وسيلة للسرقة والتزوير وتقليد المنتجات:

وفقًا لتقرير صادر عن شركة الخدمات البريطانية المتعددة الجنسيات "G4S"، فإنه من الممكن استخدام تقنية الطباعة ثُلاثيَّة الأبعاد في عمليات السرقة، عن طريق خلق نسخ مزيفة من الأختام والمفاتيح، خاصة بعد تمكن اللصوص من سرقة شحنة أدوية في عام 2015 باستخدام مفاتيح وهمية تمت طباعتها في مدة لا تزيد على 10 عشر دقائق، وفقًا لتقرير منظمة SpedLogSwiss للخدمات اللوجستية[4].

1- Sarah Anderson Goehrke, UK Police Note Potential for 3D Printing Uses in Terrorist Activity, 3dprint, url: https://bit.ly/2RcaC1f
2- tim Adams, The ‹chemputer› that could print out any drug, Theguardian, url: https://bit.ly/2v-291jd
3- Craig Schwartz, Op.cit.
4- Fake 3D printed security seals are helping thieves steal cargo, warns G4S, 3ders, url: https://bit.ly/2SsRrOf

وليس هذا فحسب، بل يمكن استخدامها في تقليد المنتجات الأصلية، مما يعتبر انتهاكًا لحقوق الملكية الفكرية، وتزوير التحف الفنية والتماثيل وغيرها.

سادسًا: البيانات العملاقة

تُعَدُّ البيانات الضخمة أو العملاقة الثروة الحقيقية في مُجتمع ما بعد المعلومات، والمغذي الرئيسي لجميع التقنيات الذَّكيَّة، فهي بمثابة الدم الذي يجري في الأجساد البشرية، ومن دونها لا يمكن تصميم تقنيات الذَّكاء الاصطناعي والرُّوبوتات والمركبات ذاتية القيادة، ويصعب تحليل احتياجات الأشخاص وتوجهاتهم لتقديم خدمات ذكية أفضل لهم، ويستحيل إنشاء مدن ومُجتمعات ذكية تتسم بالكفاءة والفاعلية في إدارة الموارد. وبإيجاز فإن البيانات العملاقة هي الروح الحقيقية للتقنيات الذَّكيَّة، وفي عام 2012 حددت الحكومة البريطانية البيانات الضخمة بوصفها واحدة من ثماني تقنيات مستقبلية عظيمة.

1- المقصود بالبيانات العملاقة:

تُعَدُّ البيانات Data هي الصورة الخام للمعلومات قبل عمليات الفرز والترتيب والمعالجة، ولا يمكن الاستفادة منها بصورتها الأولية قبل المعالجة. أما المعلومات Information فهي البيانات التي خضعت للمعالجة والتحليل والتفسير، والتي يمكن الاستفادة منها في استنباط العلاقات المختلفة بين الظواهر واتخاذ القرارات.

ويمكن تقسيم البيانات الخام إلى ثلاثة أنواع رئيسية، هي[1]:

- **بيانات مهيكلة:** هي البيانات المنظمة في صورة جداول أو قواعد بيانات تمهيدًا لمعالجتها.

- **بيانات غير مهيكلة:** تشكل النسبة الأكبر من البيانات، وهي البيانات التي يولدها الأشخاص يوميًّا من كتابات نصية وصور وفيديوهات ورسائل ونقرات على مواقع الإنترنت وغيرها.

1-Jean Louis Monino, Soraya sedkaoui, Big Data, Open Data, and Data Development, volume 3, wiley 2016. P xv

- **بيانات نصف مهيكلة:** تجمع بين بعض خصائص البيانات المهيكلة وغير المهيكلة أيضًا، بصورة يصعب تصنيفها مع أي منهما.

ويُقصد بوصف "العملاقة" أو "الضخمة" - وفق معهد ماكنزي - أنها "أي حجم يفوق قدرة أدوات قواعد البيانات التقليدية من التقاط، وتخزين، وإدارة وتحليل تلك البيانات[1]. وحتى تكون البيانات ضخمة يجب توفر ثلاثة عوامل رئيسية[2]، أو ما يُشار إليها اختصارًا بـ V3، وهي:

- **الحجم Volume:** هو عدد التيرابايت من البيانات التي يطلقها الأفراد يوميًّا من المحتوى.

- **التنوع Variety:** هو تنوع هذه البيانات ما بين مهيكلة، وغير مهيكلة، ونصف مهيكلة.

- **السرعة Velocity:** هي مدى سرعة تواتر حدوث البيانات، فمثلًا تختلف سرعة نشر التغريدات عن سرعة مسح أجهزة الاستشعار عن بُعد لتغييرات المناخ.

ويصف مفهوم البيانات العملاقة Big Data الحجم الكبير من البيانات، سواءً كانت مهيكلة، أو غير مهيكلة، وفي الحقيقة ليس الحجم هو المهم، بل ما يمكن استنباطه من هذه البيانات، أو كيف يمكن أن تستفاد جهة ما من هذه البيانات لتحسين عملية اتخاذ القرار أو تطوير أداء منتجات ذكية أو فهم احتياجات السوق والعملاء بصورة أعمق وأدق، أو إدارة الحياة اليومية في المدن

1- Big data: The next frontier for innovation, competition, and productivity, McKinsey Global Institute, May 2011, p1, available on https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Big%20data%20The%20next%20frontier%20for%20innovation/MGI_big_data_exec_summary.ashx

2- Edd Dumbill, Volume, Velocity, Variety: What You Need to Know About Big Data, FORBES, Jan 19, 2012, ACCESSED Oct 10, 2018 on https://www.forbes.com/sites/oreillymedia/2012/01/19/volume-velocity-variety-what-you-need-to-know-about-big-data/#41ecae401b6d

الذَّكيَّة من نظم إنارة للشوارع، ونظم إدارة المرور، ونظم جمع القمامة وتدوير المخلفات، وغيرها.

ويُقصد بمفهوم البيانات العملاقة أنها "تلك البيانات التي يتم الحصول عليها نتيجة خلق علاقات بين مصادر مختلفة للمعلومات، مثل المعاملات المالية ومُحرِّكات البحث وشبكات التواصل الاجتماعي، والمجسَّات Sensors والمعلومات الناتجة من تواصل الآلات مع بعضها البعض عبر إنترنت الأشياء، وهذه المعلومات يتم تخزينها وتحليلها عبر برامج عملاقة Software تعمل على إعادة تصنيف هذه المعلومات، وإنشاء روابط بينها وبين بعضها البعض، بهدف المساعدة في فهم وتطوير جميع أبعاد الظاهرة محل الاهتمام"[1].

إن أحد الأركان الرئيسية للتحول من "مجتمع المعلومات" إلى "مجتمع مابعد المعلومات" هو الانتقال من مرحلة البيانات الضخمة إلى مرحلة البيانات الصغيرة والحيوية، في عملية تهدف إلى استنباط وتحليل البيانات العملاقة بدقة عالية، حتى يتم التوصل لمعلومات أقل تساعد في فهم المستقبل وتفضيلات الأفراد بصورة أفضل، ولكن ثمة إشكاليات قانونية تواجه الشركات التكنولوجية، تتعلق بالتداخل بين المعلومات الخاصة للأفراد وبين المعلومات المطلوبة لتوفير الخدمات واحتياجات الأسواق.

2- نماذج للبيانات العملاقة:

لدى موقع "فيسبوك" الذي انطلق في عام 2004 نحو ملياري مُستخدم - ما يُعادل ربع عدد سكان العالم حاليًا - منهم 1.5 مليار مستخدم نشط. ويوميًّا يُضاف إلى هذا الموقع نحو 2.5 مليار محتوى (أي ما يُعادل 500 تيرابايت من البيانات)، وهي كمية ضخمة جدًّا، يتطلب تحليلها أدوات برمجية خاصة لتعظيم الاستفادة منها في تقديم خدمة وحلول تقنية وإعلانية أفضل لجمهور الفيسبوك.

1 -Big Data: What it is and why it matters, SAS, accessed 12 Feb 2016 on http://www.sas.com/en_us/insights/big-data/what-is-big-data.html

كما تحتاج نظم الذَّكاء الاصطناعي إلى كمية كبيرة جدًّا من البيانات العملاقة المتدفقة التي يتم تحليلها من أجل تدريب الآلات وتعليمها. ولمَّا كانت الصين تمتلك عدد سكان يفوق مليارًا و400 مليون نسمة، مع عدم وجود أي قوانين تحمي الخصوصية الشخصية للأفراد، فإن الشركات الصينية، التي تدعمها الحكومة المركزية، تستطيع الاستفادة من هذه البيانات في تحقيق نتائج متقدمة في مجال تعلم الآلات والذَّكاء الاصطناعي، فنظم المُراقبة الشاملة التي تجعل جميع أنشطة الأفراد عبر الإنترنت مُراقبة من الاتصالات الهاتفية وحركات البيع والشراء وتبادل الملفات وأي نشاط رقمي داخل الصين، وبغض النظر عن الجوانب الأخلاقية في هذه القضية؛ فإن ذلك يساعد الصين في إنشاء نظم ذكاء اصطناعي عملاقة تجعلها في مقدمة الدول الرائدة في هذا المجال، على عكس الدول الغربية التي تشاركها في السباق نفسه، والتي ينظمها إطار قانوني يحمي الخصوصية الفردية ويفرض قيودًا على عملية استخدام وتوظيف بيانات المستخدمين.

وهناك أيضًا موقع Amazon.com الذي يعالج ملايين العمليات الخلفية كل يوم، فضلًا عن استفسارات من أكثر من نصف مليون بائع وطرف ثالث. وتعتمد أمازون على نظام "اللينوكس" بشكل أساسي ليتمكن من التعامل مع هذا الكم الهائل من البيانات، وتملك أمازون أكبر 3 قواعد بيانات لينوكس في العالم، والتي تصل سعتها إلى 7.8، 18.5 و24.7 تيرابايت.

وتعالج سلسلة متاجر Walmart أكثر من مليون معاملة تجارية كل ساعة، يتم استيرادها من قواعد بيانات يُقدَّر أنها تحتوي على أكثر من 2.5 بيتابايت (2560 تيرابايت) من البيانات، وهو ما يُوازي 167 ضعف البيانات الواردة في جميع الكتب الموجودة في مكتبة الكونجرس في الولايات المتحدة. وتقوم شركة Windermere Real Estate باستخدام إشارات GPS مجهولة مما يقرب من

100 مليـون سـائق لمسـاعدة مشـتري المنـازل الجـددة لتحديـد أوقـات قيادتهـم مـن وإلى العمـل خـلال الأوقـات المختلفـة لليـوم[1].

وقـد يكـون التَّحـوُّل الرئيسـي في "مُجتمـع مـا بعـد المعلومـات" هـو الانتقـال مـن مرحلـة البيانـات الضخمـة إلى مرحلـة جديـدة أخـرى، وهـي مرحلـة البيانـات الضئيلـة أو Tiny Data، وهـي العمليـة اللاحقـة لتحليـل البيانـات الكبيـرة، والتـي تسـتهدف الحصـول علـى أهـم المعلومـات المطلوبـة The Most Important Data، بسـرعة، ودقـة عاليـة، وهـي في الحقيقـة بيانـات غيـر موجـودة، بـل يتـم اسـتنباطها والتوصـل إليها من خلال عملية تحليل البيانات العملاقة، والتي تساعد في فهم المستقبل بصـورة أفضـل، واتخـاذ قـرارات في الوقـت الحـالي لهـا تأثيـرات في المسـتقبل القريـب[2].

ولكن هناك إشكالية حقيقية تُثار حول البيانات العملاقة، وذلك بسبب سوء استخدام الشـركات للبيانـات الشـخصية للأفـراد؛ وهـو مـا اتضـح في فضيـة شـركة "كامبريدج أناليتكا"، والتـي ترتـب عليهـا جمـع معلومـات شـخصية عـن أكثـر مـن 87 مليـون أمريكـي أثنـاء الانتخابـات الرئاسـية، بمـا قـد يكـون تـم توظيفهـا بصـورة تسـاهم في التأثيـر علـى توجهاتهـم السياسـية، ودفعـت تلـك الفضيحـة الاتحـاد الأوروبي إلى إصدار "اللائحة العامة لحماية البيانات" General Data Protection Regulation المعروفـة اختصـارًا بـ(GDPR) في نهايـة مايـو 2018، والتـي أعدَّهـا البرلمـان الأوروبي ومجلـس الاتحـاد الأوروبي، لرسـم إطـار عمـل واضـح وقياسـي لأجل التعامل مع بيانات المستخدمين داخل الاتحاد، ليشمل القانون جميع الشـركات التـي ترغـب في التعامـل مـع مواطنـي دول الاتحـاد الأوروبي أو توجـد في أراضيـه.

1- أنمار رؤوف، ما البيانات الضخمة (Big Data)؟ ولماذا يجب أن نهتم بها؟، موقع أخبار العلوم، 31 ديسمبر 2017، تاريخ دخول 10 أكتوبر 2018، متاح على الرابط التالي: https://sci-ne.com/article/story_5571
2-Forget Big Data: How Tiny Data Drives Customer Happiness, trello, accessed 12 Feb 2016: http://blog.trello.com/forget-big-data-how-tiny-data-drives-customer-happiness/

وبموجب القانون، يحق لجميع مواطني الاتحاد الأوروبي أن يطالبوا الشركات التي تجمع معلومات عنهم، سواءً كانت في أوروبا، أو خارجها، بمعرفة مجالات استخدام هذه المعلومات، مع الحق في الحصول عليها في أي وقت أو طلب حذفها وعدم استخدامها، والشركات التي لن تستجيب لهذه الطلبات سيتم توقيع غرامات عليها قد تصل إلى مليارات الدولارات، ولكن هناك عقبات تنفيذية تقف أمام تطبيق القانون، أو تجعل منه فخًّا للشركات التكنولوجية قد تقع فيه، وذلك بسبب التداخل بين المعلومات الشخصية التي تتطلب إذنًا من الأفراد للحصول عليها، وبين المعلومات الأساسية المطلوبة للحصول على الخدمة، فمثلًا الحصول على الموقع الجغرافي للشخص قد يكون أمرًا شخصيًّا وخاصًّا، ولكنه في الوقت نفسه ضروري إذا رغب في الحصول على خدمات "خرائط جوجل"، أو خدمات "أوبر"... فهل من حق الشركة هنا أن تحصل على المعلومات أم لا؟!

سابعًا: التَّطبيقات الذَّكيَّة

التَّطبيقات الذَّكيَّة هي تطبيقات متعددة في مجالات التكنولوجيا، وتشمل تطبيقات الهواتف الذَّكيَّة ونظم توقع احتياجات العملاء، وغيرها، والتي يمكن توضيح أبرزها في التالي:

1- تطبيقات الهواتف الذَّكيَّة:

تمثل تطبيقات الهواتف المحمولة، أحد أهم القوى المحركة لنطاقات تفاعلات الأفراد في المنزل والعمل، وحتى تفاعلهم مع العالم بأكمله، فمن خلال تطبيقات الهاتف المحمول، يتمكن الفرد من إجراء عديد من تفاعلاته اليومية، ليس فقط التواصل مع أصدقائه عبر تطبيقات التواصل الاجتماعي، ولكن يمكن أيضًا التسوق الكامل بداية من شراء الأطعمة والملبوسات إلى المنازل والسيارات، وذلك كله عبر تطبيقات الهواتف الذَّكيَّة، حيث سهلت عديدًا من المهام على الأفراد مثل شراء منتج أو الحصول على خدمة حكومية أو استشارة طبية أو دورات تعليمية أو طلبات منزلية متعددة.

وهذا التوجه لم يكن لدى الأفراد فقط، بل لدى الشركات والحكومات أيضًا، حيث ساهمت التَّطبيقات الذَّكيَّة في تغيير طريقة تفاعل الفرد اليوم مع محيطه، سواءً في علاقته بحكومته، أو علاقته بشركته، أو علاقة الفرد بمنزله، أو علاقة العميل بالسوق الاستهلاكية. وعلى الرغم من أن هذا الاتجاه ليس حديثًا، تزداد وطأته عامًا بعد عام، ويتضح تأثيره بصورة جلية لجميع المستخدمين.

2- نظم الرد على استفسارات العملاء:

غالبًا ما يحتاج أحد المستخدمين إلى الحديث مع قسم الدعم الفني أو خدمة العملاء عبر الدردشة المباشرة Live Chat من خلال المواقع الإلكترونية للشركات، والتي تقدمها شركات، مثل "مايكروسوفت"، و"نورتون"، و"آي بي إم"،

وغيرها من الشركات، حيث يقوم المستخدم بطرح أسئلته عبر نافذة الدردشة، ومن ثم يتلقى إجابات من قسم الدعم الفني، ولكن في الحقيقة ليس جميع هذه الشركات لديها موظفون للرد على أسئلة العملاء، حيث طورت بعض هذه الشركات نظمًا ذكية قادرة على تحليل أسئلة العميل والرد عليها بما يحقق غايته ورضائه، دون أن يدرك العميل أنه يتحدث مع نظام ذكاء اصطناعي وليس ممثل خدمة عملاء[1]، كما طورت شركة "جوجل" مساعدًا يسمى «دوبلكس»، وهي تقنية مصممة لإجراء المكالمات الهاتفية نيابةً عن المستخدم، فإن كنت لست في مزاج للاتصال بالمطعم لحجز طاولة أو بصالون حلاقة لحجز موعد، يستطيع المساعد "دوبلكس" القيام بذلك.

3- نظم إدارة احتياجات العملاء:

طور عديد من الشركات تقنيات ذكية من شأنها توقع احتياجات العميل بناءً على خبراته الشرائية أو حالته الصحية، فمثلًا طورت كل من "أمازون" و"تارجت"، وهما من كبريات شركات التجزئة في الولايات المتحدة الأمريكية، نظام ذكاء قادرًا على التنبؤ باحتياجات العميل، وذلك وفق تحليل البيانات العملاقة الخاصة بتاريخه الشرائي[2]، ومن ثم تقوم بإرسال ترشيحات من منتجات أخرى إلى منزله قد تتلاءم واحتياجاته المستقبلية، كما طورت Netflix نظام ذكاء اصطناعيًّا قادرًا على ترشيح الأفلام لعملائه بناءً على اختياراتهم السابقة[3].

ليس ذلك فحسب، بل نجحت "أمازون" في إنشاء متجر "أمازون جو"، وهو أول متجر تجزئة كامل من دون طوابير للدفع، فكل ما على العميل القيام به عند

1- 10Examples of Artificial Intelligence You're Using in Daily Life, Beebom, September 16, 2016, on http://beebom.com/examples-of-artificial-intelligence/

210-1Examples of Artificial Intelligence You're Using in Daily Life, Beebom, September 16, 2016, on http://beebom.com/examples-of-artificial-intelligence/

3-The New Eyes of Surveillance: Artificial Intelligence and Humanizing Technology, Wired, accessed 23 Jan, 2017 https://www.wired.com/insights/2014/08/the-new-eyes-of-surveillance-artificial-intelligence-and-humanizing-technology/

دخول المتجر فقط تسجيل دخول بالحساب الخاص به على موقع "أمازون"، وأخذ ما يلزمه من المتجر والخروج بهدوء، بينما يقوم عديد من المستشعرات والكاميرات بالتعرف على العميل وتحديد الأصناف التي اشتراها المستهلك، وفي النهاية تأتي له فاتورة الحساب على الهاتف بكل سهولة ويسر، ويتم خصمها من حسابه البنكي.

4- الأسواق الافتراضية:

أصبح التسوق الإلكتروني سمة هذا العصر بصورة رئيسية، حيث انتشرت مواقع الإنترنت التي تقوم ببيع المنتجات بالتجزئة في عدد كبير من الدول. ومن المتوقع أن يستحوذ قطاع التجارة الإلكترونية على نسبة 15.5% من إجمالي مبيعات التجزئة في العالم في عام 2020، بحيث يصل إلى 4 تريليونات دولار، مقارنة بـ 1.6 تريليون دولار في عام 2016[1].

واحتكرت شركة "أمازون" وحدها 43% من إجمالي تجارة المبيعات الإلكترونية في الولايات المتحدة الأمريكية في عام 2016[2]، وتعتبر أكبر الشركات العاملة في مجال قطاع التجزئة على الإنترنت، حيث بلغت قيمتها السوقية نحو 355.9 مليار دولار أمريكي في العام نفسه، متفوقة في ذلك على أكبر منافسيها في المجال، وهي شركة "وول مارت"، التي بلغت قيمتها السوقية 212.4 مليار دولار في عام 2016[3].

1- Online-Shopping and E-Commerce worldwide: Statistics & Facts, https://www.statista.com/topics/871/online-shopping/
2- Amazon accounts for %43 of US online retail sales, Business Insider, Feb. 3, 2017, accessible at: http://www.businessinsider.com/amazon-accounts-for-43-of-us-online-retail-sales-2017-2(Last accessed: 9 April 2017).
3- The Extraordinary Size of Amazon in One Chart, Visual Capitalist, December 30, 2016, accessible at: http://www.visualcapitalist.com/extraordinary-size-amazon-one-chart/(Last accessed: April 10, 2017)

5- زراعة شرائح إلكترونية في الأجساد البشرية:

تمثل زراعة شرائح إلكترونية في الأجساد البشرية أحد ملامح "مُجتمع ما بعد المعلومات" والثَّورة الصِّناعيَّة الرَّابعة، ويجري العلماء في مجالات مختلفة تجارب مختلفة كي تقوم هذه الشَّرائح بعديد من المهمات الرئيسية، ومنها أنه يمكنها أن تحل محل بطاقات الائتمان أو البصمة الشخصية لدخول الأماكن أو بطاقات ركوب المواصلات العامة، أو استخدامها في مُراقبة الموظفين داخل العمل، أو مُراقبة الأطفال خارج نطاق المنزل. كما يمكنها أيضًا أن تحل محل أوراق الهوية وإثبات الشخصية لكي تكون هويات إلكترونية عبر هذه الشَّرائح، فضلًا عن استخدامها في متابعة الحالة الصحية للمرضى ومُراقبة المؤشرات الحيوية لهم، وغيرها من الاستخدامات المختلفة.

ولكن تظل المشكلة الأكبر في التداعيات التي تنجم عن ذلك، خاصة ما يتعلق بخصوصية الأفراد وضمان حريتهم الشخصية، فشريحة إلكترونية تكون كفيلة بدراسة ملامح الحياة اليومية للفرد، وإرسالها للشركات المصنعة التي قد توظف هذه المعلومات في أغراض غير مخصص لها.

6- استخدام "فوتونات" الضوء لنقل البيانات عبر الإنترنت:

استطاع علماء في مختبر "تالين" بدولة إستونيا نقل المعلومات عبر استخدام تكنولوجيا اللاي فاي ، حيث تعتمد هذه التكنولوجيا على نقل البيانات من خلال فوتونات الضوء، والفوتون في الفيزياء هو حزمة من الطاقة الكهرومغناطيسية تشكل الضوء الذي نعرفه، ومن المعروف أن أقصى سرعة هي سرعة الضوء، وأن الضوء يسير في حزم متصلة.

وبالتالي إذا تمكَّنا من وضع البيانات عبر هذه الحزم الضوئية، فإننا سنحصل على سرعة فائقة لعملية نقل البيانات، وهو ما حدث بالفعل؛ حيث نجح

العلماء داخل المختبر من استخدام تكنولوجيا "اللاي فاي" في تشغيل إنترنت بسرعة فائقة تفوق سرعة Wi-Fi الحالية 100 مرَّة، وبصورة تمكننا من تحميل 224 جيجا من البيانات في ثانية واحدة[1].

7- التواصل عبر التخاطر الذهني بين الأفراد:

نجح علماء من جامعة هارفارد في سبتمبر 2014 في إجراء أول تجربة للتواصل من خلال التخاطر الذهني Telepathy، حيث جلس أحد الأفراد في مدينة مومباي بالهند، ووضع على رأسه سمَّاعة لا سلكية متصلة بالإنترنت، وجلس آخر في باريس بفرنسا، وبمجرد أن فكَّر الأول في إلقاء التحية، ودون أن ينطق بكلمة، أدركها الشخص الآخر، فقط من خلال توارد الأفكار والخواطر.

وهذه عملية ليست بالتنجيم أو السحر، ولكن يتم استغلال الموجهات والنبضات الكهرومغناطيسية التي يرسلها المخ نتيجة عملية التفكير، ثم يحولها إلى إشارات يمكن إرسالها عبر الإنترنت، ويتم استقبالها من الطرف الآخر، وتحويلها إلى موجات يستطيع الدماغ البشري ترجمتها وفهمها[2].

8- إنتاج أدوات قادرة على تجميع نفسها ذاتيًّا:

إذا كانت الطابعات ثُلاثيَّة الأبعاد بدأت في غزو الأسواق، وأصبح من اليسير الحصول عليها في كثير من الدول، التي تستطيع طباعة مكونات مادية مثل الأطعمة والأعضاء البشرية والأسلحة وبناء المنازل وهياكل السيارات وبعض أجزاء صواريخ الفضاء، فإن هناك بعض التجارب التي تعمل على إنشاء طابعة رباعية الأبعاد 4D Printer.

1- LiFi internet: First real-world usage boasts speed 100 times faster than WiFi, IBTimes, 23 Nov 2015, Accessed 17 Feb 2016 on https://bit.ly/1NoKzgq

2-Scientists claim ‹telepathy› success after sending mental message from one person to another 4,000 miles away, Daily Mail, 6 September 2014, Accessed 20 Feb 2016. ON https://dailym.ai/2EPahuT

ولعل البعد الرابع المقصود به في هذه الطابعة هو الزمن؛ حيث تعتمد هذه الطابعة على تكنولوجيا النانو في بناء أدوات مبرمجة تعمل على تجميع نفسها ذاتيًّا Self-Assembly، حيث إن مشكلة الطابعة الثلاثية هي بناء الهياكل من خلال طبقات، ثم إعادة تجميها، بينما تعمل الطابعة رباعية الأبعاد على إنشاء هياكل ذكية قادرة على تجميع نفسها بصورة ذاتية[1]، ويعتبر المشروع في بدايته، حيث تم إنتاج مجسمات وأشكال أولية قادرة على تجميع نفسها، وليس منتجات نهائية.

9- تخزين ملايين الوثائق داخل الDNA:

يعتبر DNA هو أقدم وسيلة لتخزين البيانات في التاريخ لما يتميز به من قدرة على نقل البيانات والمعلومات الوراثية الخاصة بالكائنات الحية من جيل إلى آخر. وقد طور الباحثان "جورج تشرتش" و"سري كوسوري" في علم الجينات في جامعة هارفارد، خصائص DNA لتصبح قادرة على تخزين المعلومات الرقمية، حيث تمكَّنا في عام 2011 من تخزين النسخة الرقمية لكتاب كامل مؤلف من 300 صفحة تعادل نحو 700 تيرابايت (الف جيجا بيت) على مواد مصنوعة من جرام واحد من الحمض النووي[2].

كما نجح علماء في جامعة كامبريدج في تخزين المجموعة الكاملة لأسطوانات شكسبير ال154 داخلDNA[3]، حيث يتمكن جرام واحد فقط من DNA من تخزين 455 مليار جيجابيت (إيجزابيت) مدى الحياة[4]، ولذا يُثار التساؤل: هل يصبح جسد الإنسان في المستقبل وسيطًا لتخزين البيانات؟!

1- The emergence of «4D printing», Ted, Feb 2013, Accessed 11 Feb 2016, on https://bit.ly/1Rwaqkw

2- الحمض النووي ذاكرة المستقبل، جريدة الخليج، تاريخ نشر 2 يناير 2013، تاريخ المطالعة 21 فبراير 2016، للمطالعة على: https://bit.ly/2RanJAd

3- Shakespeare and Martin Luther King demonstrate potential of DNA storage, The Guardian, 24 Jan 2013, Accessed 16 Feb 2016 on https://bit.ly/2PWRbov

4-The eternity drive: Why DNA could be the future of data storage, CNN, 25 Feb 2015, Accessed 13 Feb 2016, on: https://cnn.it/1GuWAcx

وتتم عملية عملية تخزين البيانات داخل DNA من خلال تحويل لغة النظام الثنائي Binary System الذي يتم به تخزين البيانات في صورتها الرقمية على أجهزة الكمبيوتر، إلى نظام الأبجديات الذي يتم تخزين البيانات داخل الحمض النووي من خلاله، والتي تأخذ شكل أحرف ACTG، ثم طباعتها وتوليفها على أجزاء من الحمض النووي وتخزينها[1]، فمثلاً يتم تحويل معلومات رقمية على شكل 11101001 إلى TTCAGTTCGAACT.

ويمكن للباحثين باستخدام ما يُسمى منظم DNA، إعادة قراءة البيانات التي طبعت على الـ DNA بعد توليفها وإعادة تنظيمها مرَّة أخرى في شكل رقمي. ومع ذلك فإن الجانب السلبي في تلك التقنية هو تكلفته اﻻمرتفعة، ولكن يتوقع العلماء أن تنخفض تلك التكلفة خلال 10 سنوات بشكل كافٍ، ما يسمح بتخزين أهم وأكبر قدر ممكن من بياناتن الخاصة[2].

10– إمكانية وصول الفضاء عبر مصعد كهربائي:

نجحت إحدى الشركات الكندية، وهي Thoth Technology في إنشاء تقنية جديدة لصعود الفضاء، هي "المصعد الفضائي"، وهو عبارة عن مصعد بارتفاع 20 كيلومترًا، أي ما يعادل أكثر من 20 مرَّة قدر ارتفاع برج خليفة بدولة الإمارات العربية المتحدة، وهو أطول برج في العالم، حيث يعمل هذا المصعد على توصيل الأقمار الصِّناعيَّة ومركبات الفضاء إلى الغلاف الجوي، بما يخفض تكلفة صناعة الفضاء إلى الثلث بفضل خفض استهلاك الوقود.

ووفقًا لهذا الاختراع، سيتم إطلاق مركبات الفضاء من سطح المصعد، ويمكنها أن تعود إليها مرَّة أخرى للتزود بالوقود وإكمال مهمتها في الفضاء

1-https://bit.ly/2RanJAd
2-https://bit.ly/2RhW14M

من جديد، وهو ما يعمل على خفض التكلفة[1]. ومع ذلك لم يتم إنتاج هذا المصعد حتى الآن، بل هو أيضًا لا يزال تصميم حصلت على براءة اختراعه الشركة الكندية، ولم تكمل تنفيذه بعد.

1- مصعد فضائي بطول 20 برج خليفة، موقع روسيا اليوم، 17 أغسطس 2015، تاريخ دخول 20 فبراير 2016، للمطالعة: https://bit.ly/2Cuspc0

الفصل الثَّالث

التهديدات الأمنية للتقنيات الذَّكيَّة في "مُجتمع ما بعد المعلومات"

> لقد أصبح من الواضح بشكل مروع أن تقنياتنا تجاوزت إنسانيتنا
>
> ألبيرت أينشتين

تتعدَّد مصادر تهديد الأمن القومي في ظل "مُجتمع ما بعد المعلومات"،فهناك تهديدات مباشرة ذات تأثير عالٍ واحتمالية حدوث عالية، ومنها "الهجمات السيبرانية Cyber Attacks" التي قد تأخذ عدة أشكال أكثر تطورًا من مجرد هجمات، وذلك مثل الحروب السيبرانية Cyber warfare، التي تأتي أيضًا في إطار عدم الاستقرار السياسي، والإرهاب السيبراني، حيث تمثل هذه المجموعة مصادر للتهديد المباشر للأمن القومي للدُّول في ظل مُجتمع ما بعد المعلومات. كما أن هناك مصادر تهديد أخرى غير مباشرة تتمثل في الكوارث الطبيعية وفقدان مصادر الطاقة والتدمير المادي للخوادم. ولذلك يحاول هذا القسم إلقاء مزيد من الضوء على التهديدات التي تواجه الأمن القومي للدُّول في ظل "مُجتمع ما بعد المعلومات".

أولًا: الهجمات السيبرانية

تُعَدُّ الهجمات السيبرانية أخطر مصادر تهديد الأمن القومي في ظل مُجتمع ما بعد المعلومات، وهي تلك الهجمات التي تتم عبر شبكة الإنترنت بهدف التدمير أو التجسس أو التزييف، سواءً كانت عبر أجهزة كمبيوتر، أو هواتف ذكية، أو أجهزة إنترنت الأشياء، بل يتعدى الأمر ذلك ليشمل أيضًا الأجهزة غير المتصلة بالإنترنت مثل المولدات والمُحرِّكات، والتي يمكن تدميرها عبر فيروسات الكمبيوتر، وتكون الخسائر في هذه الحالة فادحة، خاصة إذا استهدفت البنية التحتية للدولة، من نظم اتصالات، ومواصلات، ومستشفيات، وسدود، وخزانات مياه، ومحطات طاقة، أو استهدفت سيارات ذاتية القيادة، أو درونز، أو ربوتات، تُكوِّن منها جيوشًا يمكن استخدامها في إلحاق خسائر بشرية أو مادية.

1- معايير تصنيف الهجمات السيبرانية:

تتعدَّد أنواع الهجمات السيبرانية وفقًا لعدة معايير، فقد يكون المعيار هو أسلوب تنفيذ الهجمة نفسها، أو قطاع الجمهور المُستهدَف منها، أو الهدف النهائي المرجو تحقيقه منها، أو الفواعل المشاركون فيها. ويمكن توضيح ذلك من خلال التالي:

أ- حسب الأسلوب المستخدم:

تتعدَّد الأساليب الفنية لتنفيذ الهجمات السيبرانية، ومن أبرزها ما يلي:

• **هجمات التصيد Phishing:** يعتمد هذا الأسلوب على الهندسة الاجتماعية Social Engineering من خلال تحفيز الضحية لفتح رابط يحتوي على برمجية خبيثة تصيب الجهاز، وذلك من خلال إرسال رسائل تحتوي على موضوعات قد تكون من اهتمام الضحية، أو استخدام أسماء قد تكون مألوفة بالنسبة لها، مع إرفاق إحدى البرمجيات الخبيثة بهذه الرسائل. وبمجرد قيام الضحية بفتح الرسالة تبدأ عملية القرصنة. ويُعتبر

البريد الإلكتروني والرسائل الشخصية والتَّطبيقات التي يتم تنصيبها على مواقع التواصل الاجتماعي من أكثر الأشكال شيوعًا.

• **هجمات وقف الخدمة DDOS:** هي أحد أخطر أشكال الهجمات السيبرانية، حيث يتم استخدام برامج كمبيوتر مخصصة لهذا الغرض، أو السيطرة على عدد كبير من أجهزة الكمبيوتر وتكوين شبكة روبوتية بينها تسمى Botnet، يستخدمها الهاكرز في إطلاق هجمة إلكترونية ضخمة على الضحية، وإغراقها بالآلاف من الرسائل والطلبات التي تؤدي في النهاية إلى انقطاع الخدمة ووقفها، سواء كان ذلك موقع إنترنت، أو خدمة إلكترونية خاصة، أو حكومية.

• **الثغرات الصفرية Zero-Day:** هي الثغرات الحديثة نسبيًّا، والتي لم يتم اكتشافها بعد من قبل المطورين والباحثين الأمنيين، وعادة ما تكون موجودة في برامج التشغيل وتطبيقات الكمبيوتر والهواتف الذَّكيَّة، وإذا اكتشفها أحد قراصنة المعلومات قبل الفنيين، فإنه قد يستغلها في السيطرة على أجهزة الضحايا بصورة مباشرة أو حقنها بعدد من التَّطبيقات والبرمجيات الخبيثة التي تقوم بوظائف معينة.

• **الأبواب الخلفية Backdoors:** يلجأ بعض الشركات إلى هذه الآلية بهدف الدخول على جهاز المُستخدِم بصورة مباشرة لإصلاح مشكلة فنية مثلًا أو جمع معلومات عن آلية عمل الجهاز، أو يقوم بعض المنظمات والمؤسسات الأمنية بوضعها على أجهزة الضحايا بهدف التجسس والمراقبة؛ ومن ثم فهي ليست ثغرات مجهولة، بل ثغرات مقصودة.

• **الثغرات التقنية:** هي الأخطاء التقنية التي تؤدي إلى ثغرات، مثل سوء هندسة الشبكة الداخلية الخاصة بالشركة أو المؤسسة، أو ضعف إجراءات التأمين الخاصة بها، أو الثغرات الموجودة في التَّطبيقات سيئة السُّمعة، والتي يستغلها القراصنة لإصابة الأجهزة والخوادم. ومن الأنماط التي تستخدم في ذلك نمط SQL Injection Attack.

ب- حسب القطاع المستهدف:

يمكن تصنيف الهجمات السيبرانية أيضًا وفق طبيعة الجمهور المُستهدَف منها، فقد يكونون أفرادًا عاديين يتم اختراقهم بهدف الابتزاز أو استغلال أجهزتهم مرَّة أخرى في إطلاق هجمة أعنف وأشد، أو شركات خاصة لسرقة حقوق الملكية الفكرية وبراءات الاختراع وخطط التسويق، أو القطاع المالي والمصرفي بهدف الإضرار باقتصاد الدولة أو سرقة الأموال، أو خدمات حكومية للتعبير عن الاعتراض على موقف معين، أو أجهزة أمنية بهدف سرقة معلومات استخباراتية وخطط عسكرية وتصميمات أسلحة، أو مؤسسات إعلامية بسبب موقفها من إحدى القضايا التي تشغل الرأي العام.

ج- حسب الهدف من الهجمة:

يمكن تصنيف الهجمات السيبرانية وفقًا لطبيعة الهدف منها، فقد يكون الهدف "مالي" من خلال اختراق الحسابات البنكية وبطاقات الائتمان أو اختطاف أجهزة الأفراد وطلب فدية منهم؛ أو هدف "عسكري"، مثل اختراق النظم العسكرية والطائرات من دون طيار وسرقة المعلومات الاستخباراتية؛ أو هدف "سياسي" للتعبير عن الغضب من قرارات أو تصرفات سياسية؛ أو هدف "إنساني" للتعبير عن التعاطف مع قضية إنسانية مثلًا كاختراق المواقع الإسرائيلية تعاطفًا مع القضية الفلسطينية؛ أو حتى لهدف "دعائي" مثل اختراق مواقع الشركات الكبرى بهدف إظهار القدرات والاستعراض.

د- حسب الفواعل المشاركة:

قد يقوم بهذه الهجمات "قوات مسلحة" وجيوش إلكترونية في إطار الصراعات العسكرية والسياسية بين الدول وبعضها البعض، أو "مجموعات إجرامية" وعصابات منظمة من أجل السرقة وغسيل الأموال، أو "جماعات إرهابية" كأحد

أنواع ممارسة الإرهاب الإلكتروني، أو مجموعات قرصنة عادية لأسباب مختلفة، قد تكون بهدف سرقة أموال أو التعبير عن غضب أو إرسال رسالة محددة... إلخ.

2- أنواع قراصنة المعلومات:

في الحقيقة فإن الهاكرز أو قراصنة المعلومات أقسام وأنواع وتخصصات ومستويات، ولكل واحد منهم درجته في "سوق الهاكرز" وسعره، بناءً على خبراته ومؤهلاته وسيرته الذاتية. ولعل التصنيف التقليدي للهاكرز هو:

- **الهاكر ذو القبعة البيضاء White Hat Hacker، أو الهاكر الأخلاقي Ethical:** هو ذلك الشخص الذي يستخدم قدراته في مجال الكمبيوتر بصورة شرعية لا يترتب عليها الإضرار بمصالح الغير، ويحاول أن يجد الثغرات في أنظمة الكمبيوتر بهدف تأمينها من محاولة الاختراق الخارجية. وعادة ما يلجأ كثير من الدول إلى تجنيد هذا النوع من القراصنة، بما يمتلكونه من قدرات متقدمة في مجال استخدام التكنولوجيا الحديثة، وتحاول توظيفهم في أعمال أخلاقية وشرعية، مثل ضبط الجرائم الإلكترونية، أو تجنيدهم في القوات المسلحة في وحدات إدارة الحروب الإلكترونية Cyber Warfare.

- **الهاكر ذو القُبَّعة السوداء Black Hat Hacker، أوCracker:** هو ذلك الشخص الذي يستغل قدراته للإضرار بمصالح الآخرين، أو لتحقيق أهداف غير شرعية، كسرقة البنوك والبطاقات الائتمانية، واختراق الهواتف المحمولة ومواقع الإنترنت والشبكات، حيث يتميز بقدراته المتقدمة في استخدام أدوات الاختراق والقرصنة الإلكترونية، بهدف السرقة والتدمير والتخريب.

ويكثر وجود هذا النوع في الإنترنت المظلم، وهو جزء من الإنترنت لا يظهر على مواقع البحث، ويتطلب برامج ومتصفحات معينة لكي يمكن الولوج إليه، مثل متصفح تور TOR، الذي يتم فيه بيع كل ما هو ممنوع ومحظور قانونًا.

• **الهاكر ذو القُبَّعة الرمادية Grey Hat Hacker:** هو الشخص الذي في منزلة وسط بين الإصلاح والعبث؛ فتارة يقوم بتأمين وحماية أنظمة الكمبيوتر، وتارة أخرى يقوم باختراقه التحقيق أهداف شخصية .ولعل تلك التسميات جاءت من الأفلام الغربية القديمة، التي كان الأفراد الصالحون يرتدون القُبَّعات البيضاء، والمفسدون يرتدون القُبَّعات السوداء.

وبصورة عامة، يمكن القول إن جميع المستويات السابقة هي من الهاكرز المحترفين بصورة أساسية، والذين يتميزون بقدرات عالية ومتقدمة في قرصنة التقنيات الحديثة، وأكثر النظم الأمنية تعقيدًا، وبالتالي تكون أسعارهم في سوق القراصنة مرتفعة، ولكن هناك أيضًا درجة أقل من القراصنة، فهناك "الهاكر المنفرد" Lone Hacker، والذي يمكن تسميته أيضًا Youtube Hacker، وهو الذي يعتمد على تطوير قدراته من خلال مشاهدة فيديوهات، أو قراءة مقالات حول الاختراق، وغالبًا ما تكون قدراته محدودة تعتمد على استخدام الهندسة الاجتماعية لتحفيز الضحية على فتح رابط معين به فيروس أو برنامج ضار بما يسمى Phishing أو التصيد، ورغم أنه أشهر أنواع القرصنة البدائية، فإنه من أكثر الأنواع خطورة لأنه يعتمد على إثارة الميول الشخصية للضحية بهدف الإيقاع بها.

ونتيجة لكثرة الأنظمة الإلكترونية وتعددها، ما بين نظم مالية خاصة بالمؤسسات المالية والبنوك، وأخرى إدارية متعلقة بإدارة الشركات والمؤسسات، وأخرى أمنية خاصة بتأمين المعلومات وحمايتها، وأخرى استراتيجية خاصة بإدارة البنية التحتية مثل محطات الطاقة والوقود، وأخرى خاصة بنظم الملاحة وتحديد المواقع، وأخرى خاصة بالهواتف المحمولة؛ فقد خُلِقَت حاجة تلقائية لتخصص الهاكرز في أحد هذه الأنظمة بهدف تغطية جميع جوانبها.

ولذا ظهر الهاكرز المتخصصون في سرقة بطاقات الائتمان والحسابات البنكية، وآخرون وظيفتهم اختراق الإيميلات والحسابات والصفحات الشخصية على مواقع التواصل الاجتماعي، وآخرون متخصصون في تطوير فيروسات تستخدم كأسلحة إلكترونية، وعادة ما تتراوح أسعار الهاكرز في السوق السوداء بين 50 و10 آلاف دولار، وفقًا لطبيعة المهمة المستأجر لها الهاكرز وإمكانياتهم، بل أصبح هناك تخوفات من ظهور نوع جديد من القراصنة، يطلق عليهم اسم "البيوهاكرز"، أو القراصنة المتخصصين في سرقة البيانات البيولوجية الحيوية من الإنترنت.

3- مخاطر الجيل الجديد من الهجمات السيبرانية:

تميزت الهجمات السيبرانية خلال العقد الأخير بأنها هجمات محدودة ومؤقتة، لا تؤثر على قطاع كبير من المستخدمين، ولا تتسبب في شلل الإنترنت أو وقف الخدمات الحكومية بصورة كبيرة، وذلك باستثناء الهجمات التي لها طابع عسكري مثل "ستاكس نت" التي استُخدمت ضد مواقع إيران النووية لتعطيل أجهزة الطرد المركزي، حيث اقتصرت هذه الهجمات على استهداف الحسابات البنكية واختراق المواقع الإلكترونية والصفحات الرسمية على مواقع التواصل الاجتماعي، وعادة ما كانت تتسبب في شلل مؤقت للخدمة يتم تلافيه بسرعة من قبل الفنيين والمختصين.

وظل هذا الأمر، أي الهجمات المحدودة والمؤقتة، حتى جاء هجوم "إنترنت الأشياء" الذي وقع في الولايات المتحدة الأمريكية يوم الجمعة 21 أكتوبر 2016، والذي كان بمثابة تحول رئيسي في شكل ونوعية الهجمات السيبرانية، حيث تمكن بعض القراصنة من السيطرة على أجهزة بسيطة متصلة بالإنترنت، مثل بعض الألعاب الإلكترونية، وأجهزة تشغيل الموسيقى، وكاميرات متصلة بالإنترنت، وبعض الأدوات الإلكترونية المنزلية، التي تعكس حرفيًّا مفهوم

إنترنت الأشياء، واستخدامها في إطلاق هجوم إلكتروني على عديد من المواقع الإلكترونية، مثل "تويتر" و"نتفليكس"، وبعض الشركات المشغلة لنطاقات Domains المواقع الإلكترونية، مثل شركة Dyn DNS وإغراق الخوادم المشغلة للمواقع بملايين، بل بمليارات الطلبات التي تفوق قدرة الخوادم على معالجة البيانات والاستجابة للطلبات، مما تسبب في انقطاع الخدمة عن عدد كبير من المستخدمين لمدة وصلت إلى 11 ساعة[1].

وبعد هذه الحادثة بأقل من ستة أشهر، جاءت هجمات الفدية الخبيثة Ransomware التي تُعتبر أول هجمات من نوعها على هذا النطاق، وعلى هذا العدد من المستخدمين، وتسببت في خسائر مالية كبيرة، وأوقفت قطاع الصحة في بريطانيا عن العمل، وتسببت في إلغاء عديد من العمليات الجراحية وتأجيل الحالات الصحية الطارئة، فاستطاعت هذه الهجمات التأثير على قطاع كبير من المستخدمين في وقت قياسي، وتسببت في شلل لأحد أهم قطاعات البنية التحتية البريطانية، وهو قطاع الصحة، **ولذلك يمكن القول إن الجيل المقبل من الهجمات السيبرانية يتميز بخصائص معينة، منها:**

يتميز الجيل الجديد من الهجمات السيبرانية بخصائص معينة، من أبرزها: سرعة تطور شكل الهجمات، وضيق الفجوة الزمنية بين تنفيذ هجمات كبرى، والاعتماد على "البيتكوين" كأساسٍ للهجمات، وتصاعد حدة وشدة الهجمات وصعوبة تحديد مصدرها وتعقبه، وعدم توقع التداعيات السلبية للهجمات التي تستهدف البنى التحتية الحرجة، ومزيد من مشاركة الفواعل من دون الدول خاصةً من القراصنة العاديين وأفراد الجماعات الإرهابية والجريمة المنظمة، ومشاركة غير الفنيين نظرًا لتوافر العديد من برامج القرصنة الإلكترونية.

1- Julia Franz ,October's cyberattack used the ‹internet of things› to attack the internet itself. Here's why it could happen again, November 13, 2016, on: https://www.pri.org/stories/2016-11-13/october-s-cyberattack-used-internet-things-attack-internet-itself-here-s-why-it

أ- سرعة تطور شكل الهجمات السيبرانية:

يتطور في هذا الجيل شكل الهجمات السيبرانية بصورة سريعة، فقد يكون مرَّة عبر أجهزة الحاسب، ومرَّة عبر إنترنت الأشياء، ومرَّة عبر أجهزة الهواتف المحمولة. ومستقبلًا قد يكون عبر نظم الذَّكاء الاصطناعي والروبوت، بحيث يستهدف في أحدها الأموال، وفي مرَّة أخرى الاعتراض السياسي أو الارهاب، وفي غيرها العنف غير المبرر.

ب- ضيق الفجوة الزمنية بين الهجمات الكبرى:

يكون الفارق الزمني بين هجمة سيبرانية، وغيرها، قصيرًا جدًّا، فيمكن أن نشهد عدة هجمات كبرى خلال عام واحد، فما يكاد العالم يخرج من تداعيات هجمة حتى تظهر له غيرها، مختلفة في الآلية والنطاق والجمهور.

ج- الاعتماد على العُملات الافتراضية:

في هذا الجيل تصبح "البيتكوين" أساس الهجمات، وذلك لأنها صعبة التعقب، وليس لها إدارة مركزية، ومع ذلك يمكن البيع والشراء من خلالها، أو حتى تحويلها إلى عُملات تقليدية من خلال ماكينات الصرف الآلي المنتشرة في دول متعددة، فتصبح العملة الرسمية للهجمات السيبرانية.

د- زيادة درجة تعقيد الهجمة وتداعياتها:

تكون الهجمات معقدة في طريقة تنفيذها، ويصعب تعقبها أو معرفة مصدرها، فقد يشارك فيها عدد كبير من الأفراد حول العالم، وتستخدم أجهزة غير متوقعة في عملية القرصنة، مثل الطائرات من دون طيار من أجل التضليل، وتكون تداعياتها لا تحتمل على مستوى الأفراد أو الدول.

هـ- دور بارز للفواعل من غير الدول:

يلعب الفواعل من دون الدول دورًا مهمًا، قد يكون مُساويًا لدور الدول، سواء كانت مجموعة قرصنة، أو حركات إرهابية، أو مافيا دولية، أو حتى أفرادًا عاديين.

و- مشاركة غير الفنيين:

تم تطوير عديد من برامج القرصنة الإلكترونية التي لا تحتاج إلى مطورين مختصين لاستخدامها، بل يمكن شراؤها واستخدامها بصورة سهلة، وهو ما يفتح الباب لقطاع كبير من غير المختصين للمشاركة في هذا النوع من الهجمات.

ومع انتشار التكنولوجيا داخل المُجتمعات، وتوجه الجيوش نحو الاعتماد على فيروسات الحاسب والأسلحة القتالية ذاتية التشغيل Autonomous Weapons، وتوجه الدول لتبني نماذج المدن الذَّكيَّة التي تعتمد بصورة رئيسية على تكنولوجيا المعلومات والاتصالات لإدارة جميع متطلبات الحياة اليومية فيها، واعتماد النظم المالية والمصرفية والإدارية على الإنترنت، وانتشار أجهزة إنترنت الأشياء في كل مكان؛ تصبح الدول والأفراد أكثر عُرضة للاختراق، وتصبح جميع الخدمات الحكومية أكثر عُرضة للتوقف المفاجئ من خلال الهجمات السيبرانية، وتصبح قواعد البيانات والخطط والاستراتيجيات والوثائق والمعلومات السرية أكثر عُرضة للتلاعب بها وتسريبها، وتصبح الأسلحة والأدوات العسكرية قليلة التكلفة وسهلة التصنيع وشديدة التدمير، فهي عبارة عن فيروسات كمبيوتر، وتزداد احتمالية نشوب صراعات سيبرانية Cyber Conflicts بين الدول لا يمكن احتواؤها، حتى إنها قد تتطور وتصل إلى مرحلة الحرب السيبرانية الشاملة.

ثانيًا: الحروب السيبرانية

يُعتبر الفاعل الرئيسي في الحروب السيبرانية هو الدول بالأساس، حيث بدأت بعض الدول الاستعداد لهذا النوع من الحروب، سواء من خلال إنشاء جيوش سيبرانية داخل صفوف القوات المسلحة للدُّول، أو من خلال إبرام الاتفاقات السياسية والعسكرية، حيث توصلت الولايات المتحدة الأمريكية والصين في عام 2015 لاتفاق خاص بالحروب السيبرانية، يقضي بعدم شن أي هجمة سيبرانية بين الدولتين على البنية التحتية وشركات القطاع الخاص في حالة السلم. كما أعلن الاتحاد الأوروبي في أكتوبر عام 2017 أن شن هجمة سيبرانية من دولة عدائية على دول الاتحاد الأوروبي يعتبر "تصرف حرب" يستوجب الدفاع عن النفس[1]، فضلاً عن تغيير العقيدة العسكرية لحلف شمال الأطلسي "الناتو" لتشمل الحرب في الفضاء الإلكتروني.

1- مؤشرات الحروب السيبرانية:

يبدو أن الحرب السيبرانية قد اقتربت بالفعل، فكل عام نشهد على الأقل معركة - أو اثنتين - تحدث عبر الفضاء الإلكتروني، وتمهد الطريق لحدوث حرب سيبرانية كبرى، مثل المعركة بين روسيا وإستونيا في عام 2007 وبين روسيا وجورجيا في عام 2008، والولايات المتحدة الأمريكية وإيران في عام 2009، ولهذا طغى مفهوم الأمن السيبراني على استراتيجية الأمن القومي البريطاني والأمريكي منذ عام 2010، وكشف "إدوارد سنودن" في عام 2012 عن تقنيات متقدمة قامت وكالة الأمن القومي الأمريكي بتطويرها واستخدامها في اختراق جميع الأفراد حول العالم بمن فيهم رؤساء الدول، وهو ما دفع المحلل والاستشاري "ريتشارد ستينون Richard Stiennon" للتحذير من حرب سيبرانية مقبلة، في

1-Phil Muncaster, EU to Declare Cyber-Attacks "Act of War", Infosecuritymagazine, 31 OCT 2017, https://www.infosecurity-magazine.com/news/eu-to-declare-cyber-attacks-act-of/

كتابه الصادر في عام 2015 تحت عنوان "سوف تكون حربًا سيبرانية There Will Be Cyberwar".

والحرب السيبرانية ليست وليدة الأمس، بل هي موجودة منذ أكثر من عقد من الزمان، مع اختلاف حدتها وأشكالها. ومن أبرز النماذج على ذلك، الهجمات السيبرانية التي شنتها الصين على الولايات المتحدة الأمريكية في عام 2001، حيث تعرَّض ما يقرب من 1200 موقع أمريكي لهجمات من قراصنة صينيين في الفترة من 30 أبريل حتى 7 مايو عام 2001، وشملت تلك الهجمات مواقع البيت الأبيض والقوات الجوية الأمريكية ووزارة الطاقة الأمريكية[1]، وذلك على خلفية اصطدام مقاتلة صينية من طراز "J-8 land" مع طائرة تجسس أمريكية من طراز "EP-3E" فوق جزيرة "هاينان" الصينية في الأول من أبريل عام [2]2001).

كما قام قراصنة صينيون بشن بضع هجمات على شركة "لوكهيد مارتين" الأمريكية، حيث سرقوا معلومات عن تكنولوجيا تصنيع مقاتلة "إف – 35" التي استخدمتها الصين فيما بعد لدى تصميم وتصنيع مقاتلة "تي 20" الصينية[3]. وشملت الهجمات السيبرانية أيضًا مقاولين لدى وزارة الدفاع الأمريكية يعملون على صناعة وتطوير الطائرات من دون طيار الأمريكية، بهدف سرقة معلومات حول هذه الطائرات وكيفية صناعتها وتطويرها[4].

1-Michael A. Vatis, Cyber Attacks During The War On Terrorism:A Predictive Analysis, Institute For Security Technology Studies At Dartmouth College, September 2001),p8

2- طائرة التجسس الأمريكية في قبضة الصين، مجلة الطيران والدفاع، عدد 35، بتاريخ دخول 20 فبراير، 2012، يمكن مطالعته على الرابط التالي: http://www.aviadef.com/article.aspx?magid=35&artid=96

3- أمريكا تتهم الصين بسرقة تكنولوجيا صنع مقاتلة «إف – 35»، روسيا اليوم، تاريخ 14 مارس 2014، بتاريخ مطالعة 20 أكتوبر 2014، يمكن المطالعة على: http://arabic.rt.com/news/668023/

4- Hacking U.S. Secrets, China Pushes for Drones, The New York Times, Sep 21, 2013, Accessed on April 17th, 2014, http://www.nytimes.com/2013/09/21/world/asia/hacking-us-secrets-china-pushes-for-drones.html?pagewanted=all&_r=2&

وقد تحدث الحرب السيبرانية ليس لأسباب عسكرية محضة، بل لمجرد الخلاف السياسي، أو بهدف سرقة المعلومات الاستراتيجية لمعرفة فيما يفكر الخصم، أو حتى سرقة تصميمات الأسلحة العسكرية والتقنيات التكنولوجية الحديثة؛ الأمر الذي دفع الولايات المتحدة إلى عقد اتفاقية مع الصين لعدم شن هجمات سيبرانية على البنية التحتية الأمريكية أو شركات القطاع الخاص في حالة السلم[1].

وتتمثل الأسلحة التي يتم استخدامها في هذه الحرب في برامج كمبيوتر تمثل فيروسات وبرمجيات خبيثة، والتي تعتبر أحد أهم عناصر إدارة الحروب السيبرانية، وهي السلاح الرئيسي الذي يتم استخدامه للقتال في هذه الحرب.

2- أبرز أشكال الأسلحة السيبرانية:

الأسلحة المُستخدمَة في الحرب السيبرانية هي فيروسات وديدان وبرمجيات خبيثة يتم تصميمها عبر أكواد وبرامج كمبيوتر، لشن هجمات إلكترونية على أهداف عسكرية ومدنية، تؤدي إلى تدمير النظم Systems، أو المكونات المادية Physical من أجهزة ومعدات أو البرمجيات Software، أو إلحاق خلل وظيفي أو فني بها[2]، بما قد يؤدي في النهاية إلى تدمير البنية التحتية للدُّول أو اختراق الأنظمة العسكرية وسرقة حقوق الملكية الفكرية وبراءات الاختراع، والتجسس على الأفراد والمعلومات وأنظمة الاتصالات، وغيرها من الأعمال التخريبية التي تهدد الأمن والسلم الدوليين[3].

1- Scott W. Harold, The U.S.-China Cyber Agreement: A Good First Step, RAND, July 31, 2016, Accessed December 14, 2017 on https://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html
2- Emilio Iasiello, Are Cyber Weapons Effective Military Tools?, Military and Strategic Affairs | Volume 7 | No. 1 | March 2015, p24 on
http://www.inss.org.il/he/wp-content/uploads/sites/2/systemfiles/SystemFiles/2_Iasiello.pdf
3 -Thomas Rid and Peter Mcburney, Cyber-Weapons, The Rusi Journal, 2012 on
http://www.tandfonline.com/doi/pdf/10.1080/03071847.2012.664354

وتتسم الأسلحة السيبرانية بعدد من المميزات تجعلها أخطر من الأسلحة التقليدية، وهي:

- **منخفضة التكاليف،** ولا تحتاج إلى معامل خاصة، وتتميز بقدرة تدميرية عالية.
- **يتم تطويرها بواسطة دول أو فواعل من دون الدول،** مثل الجماعات الإرهابية، أو حتى الأفراد.
- **تستهدف مرافق حيوية وحرجة للدولة،** سواء كانت مدنية أو عسكرية، وتسبب خسائر بشرية ومادية.
- **تسعى إما للتجسس وسرقة المعلومات أو للتدمير،** سواء تدمير وتزييف معلومات أو أجهزة ومعدات.
- **يصعب تعقب مصدرها** ومعرفة الفاعل الحقيقي الذي استخدمها في شن هجوم إلكتروني.
- **هي إحدى أهم أدوات حروب الجيل الرَّابع،** ويتم استخدامها في حالة الحرب والسلم أيضًا.

ومن أبرز أشكال الأسلحة السيبرانية ما يلي:

أ- فيروسات الحاسوب Viruses:

هي برمجيات خبيثة صُنعت عمدًا بغرض تغيير خصائص الملفات التي تصيبها لتقوم بتنفيذ بعض الأوامر إما بالإزالة أو التعديل أو الحذف أو التخريب، أي إن الغرض منها هو إلحاق الضرر، سواء كان هذا الضرر رقميًّا يتعلَّق ببرمجيات أخرى ونظم تشغيل ومعلومات، أو ماديًّا يتعلَّق بتدمير أجهزة ونظم إلكترونية.

ب- الديدان Worms :

هي برامج صغيرة لا تعتمد على غيرها وتتكاثر بنسخ نفسها عن طريق

الشبكات، وصُنعت للقيام بأعمال تخريبية كأن تعمل على قطع الاتصال بالشبكة أو سرقة بعض البيانات الخاصة بالمستخدمين أثناء تصفحهم الإنترنت، وتمتاز بسرعة الانتشار ويصعب التخلص منها، نظرًا لقدرتها الفائقة على التلون والتناسخ والمراوغة. وغالبًا عندما تُستخدَم في حروب المعلومات، فإنها تستهدف الشبكات المالية التي تعتمد على الحاسوب، مثل شبكات البنوك.

ج- أحصنة طروادة Trojan horses :

هي شفرة أو برنامج صغير مُختبئ في برنامج كبير من البرامج ذات الشعبية العالية، ويقوم ببعض المهام الخفية كأن يعمل على نشر دودة أو فيروس، وهو مبرمج بمهارة عالية؛ إذ لا يمكن اكتشاف وجوده، حيث يعمل دائمًا على مسح آثاره التي لا تحمل صفة تخريبية، وغالبًا ما يعمل على إضعاف قوى الدفاع لدى الضحية ليسهل اختراق جهازه وسرقة بياناته، كأن يقوم مثلًا بإرسال بيانات عن الثغرات الموجودة في نظام ما، وكذلك إرسال كلمات المرور السرية الخاصة بكل ما هو حساس من مخزون معلومات الطرف المستهدف.

ليس من المبالغة القول إن شن هجمات سيبرانية كبيرة تستهدف الأعمال التدميرية والتخريبية بات أحد أشكال "تصرف الحرب"، ولذا أضحى الدفاع عن النفس والرد على هذه الهجمات ودخول بعض الدول في مفاوضات للتوصل لاتفاقيات تمنعها، من العناصر الرئيسية في صياغة سياسات الأمن الوطني للدول وكذلك للأحلاف العسكرية مثل حلف شمال الأطلسي "الناتو" وكذلك لأعضاء بعض المنظمات الإقليمية مثل الاتحاد الأوروبي.

د- القنابل المنطقية :Logic Bombs

هي برمجيات يتم زرعها داخل النظام أو البرنامج الذي يطوره، أي إن المستهلك يشتري البرنامج أو الجهاز مصابًا من البداية بالسلاح السيبراني، ويتم تصميمه بحيث يبدأ العمل عند حدوث أمر معين، أو تحت ظروف معينة تمكن في النهاية العدو من السيطرة على الجهاز بصورة كاملة أو تدميره.

هـ- البرمجيات الخبيثة مثل "أريد البكاء" WannaCry:

في مايو 2017 قام مجموعة من القراصنة المجهولين بشن هجوم ضارٍ من إحدى البرمجيات الخبيثة المعروفة باسم WannaCry، وتمكن الهجوم من إصابة أكثر من 200 ألف ضحية في أكثر من مئة وخمسين دولة خلال أول 48 ساعة فقط من الهجوم[1].

وقد تميزت هذه الهجمة باستهداف الكيانات الاقتصادية، وليس الأفراد، مختلفة عما سبقها من هجمات استهدفت الأفراد بالأساس، وذلك لأن هذه المؤسسات هي الأقدر على دفع الفدية، كما أنها الأكثر تضررًا في حالة حذف بيانات العملاء، أو براءات الاختراع التي تملكها، أو حساباتها المالية، أو خططها التسويقية، أو غيرها من البيانات المهمة لها، فالخسائر التي سوف تقع على الشركات أكبر بكثير من تلك التي يمكن أن تقع على الأفراد، ومن ثم فالشركات هي الأكثر تضررًا، وبالتالي الأكثر احتمالية وقدرة أيضًا على الدفع.

والأمر المخيف في هذه الهجمة أنها اعتمدت على أسلحة إلكترونية وثغرات تم تسريبها من وكالة الأمن القومي الأمريكي؛ الأمر الذي يعكس خطورة أن تقع مثل هذه الأسلحة في يد فواعل من غير الدول، خاصة الجماعات الإرهابية، حيث أشار بعض التحليلات إلى تورط الوكالة في تطوير هذه البرمجية قبل أن تتم سرقتها منها وتسريبها.

وقد نشر موقع "ويكيليكس" تسريبات القبو 7 المعروفة باسم Vault 7 في مارس 2017، والتي سُرِّب فيها عديد من المشروعات والثغرات والبرامج التي تستخدمها وكالة الأمن القومي الأمريكي للتجسس على جميع الأراد حول العالم، وكان من بينها إحدى الأدوات التي طورتها الوكالة لاستغلال بعض

1- NHS cyberattack: Seven trusts still turning away patients, Skynews, 14 May 2017, on: https://bit.ly/2QL6upS

الثغرات الصفرية الموجودة في برامج تشغيل ويندوز للتجسس على الأفراد والحكومات، حيث قامت الوكالة بإعطاء هذه الثغرات لشركة مايكروسوفت في أغسطس الماضي، ورغم أن "مايكروسوفت" قامت بإصلاح الخلل في شهر مارس، أي قبل الهجوم بنحو شهرين، فإن التحديث لم يشمل جميع الأجهزة حول العالم، مما ترك كثيرًا منها عُرضة للهجمات. وقد استغلت هذه الثغرات مجموعة من القراصنة تطلق على نفسها لقب "وسطاء الظل" Shadow Brokers، ظهرت في عام 2016، وادعت أنها استطاعت سرقة بعض الأسلحة الإلكترونية التي قامت بتطويرها وكالة الأمن القومي الأمريكي.

و- الفيروسات الإلكترونية:

من نماذج الأسلحة الإلكترونية فيروس ستاكس نت Stuxnet، وهو أحد أخطر أنواع الأسلحة الإلكترونية التي تم اكتشافها في عام 2009، ومثل نقل نوعيَّة في خطورة الحروب الإلكترونية، فمن خلال "ستاكس نت" انتقلت الحرب من تدمير البيانات وسرقتها، إلى تدمير المكونات المادية نفسها ونظم التشغيل، وليس فقط البيانات[1]، وكذلك فيرس دوكو Duqo، وهو فيروس تم اكتشافه في سبتمبر 2011 بواسطة معمل التشفير والأمن الإلكتروني (CrySyS Lab) التابع لجامعة بودابست للاقتصاد والتكنولوجيا، وفيروس "فليم Flame الذي تم اكتشافه في عام 2012، بواسطة فريق الاستجابة والطوارئ الإيراني، فضلًا عن شركة كاسبرسكي ومعمل التشفير والأمن الإلكتروني (CrySyS Lab) التابع لجامعة بودابست للاقتصاد والتكنولوجيا، وقد أوضحت هذه الجهات أن"فيروس فلام" هو أكثر فيروس تعقيدًا تم العثور عليه، حيث أصدرت الأمم المتحدة تحذيرًا اعتبرته الأكثر خطورة من هذا الفيروس.

1- David Kushner, The Real Story of Stuxnet, IEEE institute, Feb26, 2013, accessed Jan 5, 2017m, on: https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

وفيما يلي مزيد من التفصيل حول هذه الأسلحة السيبرانية:

• **ستاكس نت Stuxnet:** تم اكتشاف هذا الفيروس في عام 2009 عندما أصاب أجهزة الطرد المركزي الإيراني، وتسبب في تعطيل وخروج عدد كبير منها عن العمل، حيث استهدف نظم تشغيل أجهزة الطرد المركزي التي تعمل عبر برنامج التحكم الصناعي SCADA من صنع شركة سيمينز الألمانية، وقام بتسجيل مؤشرات تتعلق بعملية تخصيب اليورانيوم، ثم قام بالتلاعب بآلية عمل أجهزة الطرد وتخريبها، حيث لدى "ستاكس نت" قدرة على إعادة برمجة وحدات التحكم المنطقي القابلة للبرمجة وإخفاء التغييرات التي تم تنفيذها، وفي الوقت نفسه عرض المعلومات القديمة التي قام بتسجيلها على الشاشات لكي يظهر الأمر للمراقبين والفنيين أن كل شيء يسير بصورة طبيعية، حتى نجح في إنهاء مهمته.

وبصورة عامة يقوم "ستاكسنت" بمهاجمة أنظمة التحكم الصناعي المستخدمة على نطاق واسع في المنشآت المهمة مثل خطوط نقل النفط ومحطات توليد الكهرباء والمفاعلات النووية وغيرها من المنشآت الاستراتيجية الحسَّاسة، وتقوم بالانتقال بين الأجهزة عبر أجهزة USB، مستغلةً إحدى نقاط الضعف في برنامج التشغيل ويندوز.

ليس ذلك فحسب، فقد نقلت شبكة «سي إن إن» الإخبارية الأمريكية عن "شون مكجيرك"، رئيس دائرة أمن الإنترنت في وزارة الأمن الوطني الأمريكية، قوله أمام الكونجرس: «هذا الفيروس يمكن أن يدخل تلقائيًّا لأي نظام، ويسرق صيغة المنتج الذي يتم صنعه، ويغير خلط المكونات في المنتج، ويخدع المشغلين وبرامج مكافحة الفيروسات عبر إيهامهم بأن كل شيء على ما يُرام".

• **دوكو Duqo:** هو فيروس تم اكتشافه في سبتمبر 2011 بواسطة معمل التشفير والأمن الإلكتروني (CrySyS Lab) التابع لجامعة بودابست للاقتصاد والتكنولوجيا،

وأطلق عليه لفظ Duqo نسبة إلى الملفات التي كان يقوم بنسخها، التي كانت تسمى "~DQ"، وقد تم اكتشافه في ثماني دول، هي: فرنسا، وهولندا، وسويسرا، وأوكرانيا، والهند، وإيران، والسودان، وفيتنام.

وقد تم إعداد هذا الفيروس من خلال لغة برمجة غير معروفة أو منتشرة، فلغات البرمجة في العالم متعددة والأشهر منها هو C++, Python, Ada, Lua، لكن هذا الفيروس لم يتم تحديد اللغة المستخدمة في برمجته أو التعرف عليها، لكن يعتقد أنها تعديل على لغة برمجة C بعد تطويرها، كما يعتمد تصميه أيضًا على الشفرة الرقمية لفيروس "ستاكس نت"، لذلك توجد شبهات حول علاقته بالبرنامج النووي الإيراني والتجسس على المفاوضات حول البرنامج.

وتتمثل الوظيفة الرئيسية لهذا الفيروس في التجسس على نظم التحكم الصناعي، وجمع المعلومات الاستخباراتية والاستراتيجية عن الصناعات والمرافق والبنى التحتية التي تديرها. كما أنه يقوم بوظائف فرعية أخرى في غاية الأهمية، منها إعطاء ثغرات للمبرمجين للتحكم في هذه النظم وتدميرها إذا شاؤوا، سواء تدمير البيانات والمعلومات الموجودة على الأجهزة أو حتى تدمير الأجهزة نفسها.

كما أنه يقوم بسرقة شهادات الأمان الرقمي Digital Certificates وأكواد تشغيل، وفك تشفير البرامج الرئيسية على أجهزة الكمبيوتر، بهدف إتاحة الفرصة للمبرمجين لحقن هذه الأجهزة في المستقبل بفيروسات جديدة تظهر على الكمبيوتر على أنها برامج آمنة ويصعب على برامج مكافحة التجسس اكتشافها، نظرًا لاستخدامها شهادات الأمان الرقمي والأكواد المسروقة من قبل؛ وبالتالي فهو يقوم بعملية التجسس والاستطلاع والتمهيد قبل شن الهجوم والتدمير.

ولذلك فالخطورة الناجمة عنه ليس فقط خطوة اقتصادية تتمثل في سرقة المعلومات الاقتصادية والمالية والفنية وبراءات الاختراعات وحقوق الملكية الفكرية، بل خسائر بشرية وإنسانية أيضًا تتمثل في إمكانية استخدامه في تدمير بعض المرافق الحيوية التي قد ينجم عنها خسائر في الأرواح البشرية.

• **فليم Flame:** تم اكتشاف هذا الفيروس في عام 2012، بواسطة فريق الاستجابة والطوارئ الإيراني، فضلًا عن شركة كاسبرسكي ومعمل التشفير والأمن الإلكتروني (CrySyS Lab) التابع لجامعة بودابست للاقتصاد والتكنولوجيا، وقد أوضحت هذه الجهات أن فيروس "فليم" هو أكثر فيروس تعقيدًا تم العثور عليه، حيث أصدرت الأمم المتحدة تحذيرًا اعتبرته الأكثر خطورة من هذا الفيروس، الذي استهدف دول الشرق الأوسط بالأساس، حيث تم العثور عليه في أكثر من 1000 جهاز في مؤسسات حكومية وتعليمية وأفراد في إيران، ودول أخرى، مثل مصر، وفلسطين، وسوريا، ولبنان، والمملكة العربية السعودية.

ويستطيع "فليم" القيام بعدة وظائف مختلفة على برنامج التشغيل ويندوز، تتمثل في تسجيل المحادثات الصوتية، وتسجيل جميع الأنشطة التي يتم إجراؤها عبر الكيبورد الخاصة بالكمبيوتر، وأخذ سكرين شوت من الصفحات التي يتم فتحها، وتسجيل المحادثات التي يتم إجراؤها عبر بعض برامج الدردشة مثل "سكيب"، وتحويل الجهاز المصاب إلى نقطة جمع معلومات من قبل الأجهزة الأخرى الموجودة بنفس المكان عبر فتح خاصية البلوتوث، والانتقال أيضًا إلى أي أجهزة أخرى أو وسائل نقل رقمية Flash Drive وجمع المعلومات الموجودة عليها أيضًا. كما يتميز بقدرته على محو جميع البيانات التي تمكن فرق التحقيق الرقمي من تتبع مصدره أو معرفة مكان الخادم الرئيسي الذي يتم إرسال المعلومات إليه.

ثالثًا: الإرهاب السيبراني

أصبح عديد من الدول حول العالم تعتمد على فكرة نشر واستخدام التقنيات الذَّكيَّة والجديدة، سواء داخل المؤسسات والهيئات، أو بين الأفراد وداخل المُجتمع. وتمثل إتاحة مثل هذه التقنيات سلاحًا ذا حدين، فكما يمكن استخدامه في تحسين جودة حياة البشر داخل المدينة، يمكن توظيفه أيضًا في تهديد أمن الأفراد، بل والأمن القومي للدولة؛ لذلك نجد أن بعض الدول حظرت استخدام بعض هذه التقنيات الحديثة مثل الطائرات من دون طيار، وذلك تخوفًا من استخدام الحركات الإرهابية لهذه التقنية في تنفيذ عمليات إرهابية عن بُعد، ولذلك يمثل الإرهاب السيبراني خطرًا على الأمن القومي في ظل مُجتمع ما بعد المعلومات، من خلال توظيف التقنيات الذَّكيَّة في تنفيذ عمليات إرهابية سيبرانية، سواء عبر هجمات إلكترونية في الفضاء الإلكتروني، أو استخدام الرُّوبوت والدرونز في شن عمليات إرهابية أو استخدام الطابعات ثُلاثيَّة الأبعاد في تصنيع الأسلحة.

وفيما يلي يمكن توضيح اعتماد الحركات الإرهابية على التطورات التكنولوجية، وكيف تم توظيف بعض تقنيات مُجتمع ما بعد المعلومات، مثل العُملات الافتراضية والطابعات ثُلاثيَّة الأبعاد والطائرات من دون طيار المدنية، في تنفيذ عمليات إرهابية، قد تؤدي إلى تهديد الأمن القومي للدولة عبر تهديد الحياة البشرية.

1- التقنيات الذَّكيَّة والإرهاب الإلكتروني:

تسعى الحركات الإرهابية دائمًا إلى توظيف جميع التقنيات الذَّكيَّة والتطورات التكنولوجية لتحقيق أهدافها، وتسخيرها لنشر أفكارها التقليدية بصورة متطورة وذكية تتلاءم مع مستجدات العصر، فانتقلت "الدعوة" من مرحلة شرائط الكاسيت والفيديو، إلى مواقع التواصل الاجتماعي وتطبيقات الهواتف الذَّكيَّة،

مرورًا بالمنتديات والمدونات الإلكترونية، وأصبح "التجنيد" يتم من خلال غرف الدردشة وألعاب الفيديو بعد أن كان قاصرًا على "الزوايا" والمجالس الخاصة، وتطورت "الهجمات الإرهابية" من الحزام الناسف والدراجات النارية المفخخة، إلى الهجمات السيبرانية والدرونز المسيرة، وتحولت من صناعة الأسلحة بطرق بدائية ويدوية، إلى إمكانية صناعتها عبر استخدام الطابعات ثُلاثيَّة الأبعاد، فأصبحت التكنولوجيا من أبرز أسلحة الحركات الإرهابية لتحقيق أهدافها الدعائية والعسكرية.

وقد ساهمت هذه التطورات التكنولوجية في ظهور أنماط جديدة من الإرهاب لم تكن موجودة من قبل، منها نمط الذئاب المنفردة Lowly Wolf، وهو ذلك الإرهابي الذي يعتنق الفكر المتطرف دون أن يرتبط تنظيميًّا بجماعة إرهابية، فيأخذ أفكارها المتشددة من خلال مواقع الإنترنت، ويقوم بصناعة الأسلحة من خلال الفيديوهات التعليمية الموجودة على صفحات التواصل الاجتماعي، ثم ينطلق منفردًا لتنفيذ مخططه الإرهابي.

الأسلحة السيبرانية أضحت من أهم أدوات حروب الجيلين الرابع والخامس، وهي ليست حكرًا على الدول بالطبع، إذ تقوم التنظيمات المتطرفة باستخدام بعض آلياتها؛ فهي مجرد فيروسات وديدان وبرمجيات خبيثة يتم تصميمها عبر أكواد وبرامج كمبيوتر، لشن هجمات إلكترونية على أهداف عسكرية ومدنية، تؤدي إلى تدمير النظم والبرمجيات أو المكونات المادية من أجهزة ومعدات أو إلحاق خلل وظيفي أو فني بها، بما قد يؤدي في النهاية إلى تدمير البنية التحتية للدول أو اختراق الأنظمة العسكرية والتجسس على الأفراد والمعلومات وأنظمة الاتصالات، وغيرها من الأعمال التخريبية التي تهدد أمن الدول.

وإلى جوار "الخلايا" التقليدية، ظهرت خلايا إرهابية "سيبرانية"، تنشط فقط على مواقع الإنترنت، ولا تقل مهمتها أهمية عن الخلايا التقليدية، فمنها من يقوم بعمليات الدعوة والتجنيد وجمع التمويل عبر الإنترنت، ومنها من يقوم باختراق المواقع الإلكترونية وصفحات التواصل الاجتماعي للضحايا للتأثير عليها معنويًّا، ومنها من يقوم بشن هجمات إلكترونية على بنوك ومؤسسات مالية بهدف

السرقة والحصول على المال، أو على مؤسسات سياسية وعسكرية لجمع معلومات استخباراتية لتنفيذ العمليات الإرهابية، أو تسريب وثائق ومعلومات استراتيجية، فضلًا عن استهداف خدمات الحكومات الإلكترونية والذَّكيَّة عبر الإنترنت ووقفها أو استهداف البنية التحتية للدولة وأنظمتها المالية والمصرفية والاتصالية والعسكرية، وغيرها.

2- نماذج توظيف الحركات الإرهابية للتقنيات الذَّكيَّة:

تتعدَّد استخدامات التنظيمات الإرهابية للتكنولوجيا ومخرجاتها، سواءً لأغراض التجنيد والدعاية الدينية المتطرفة، أو للتمويل من مصادر خفية يصعب تعقبها، أو في صناعة الأسلحة وتنفيذ العمليات الإرهابية. **ومن أبرز التكنولوجيات الجديدة التي توظفها هذه التنظيمات ما يلي:**

أ- الدرونز المدنية:

تُعتبر الطائرات من دون طيار، أو الدرونز "المدنية"، والمخصصة للأغراض التجارية والترفيهية، سلاحًا ذا حدين، فكما يمكن أن تستخدم في توصيل الطلبات ومُراقبة المحاصيل الزراعية أو التصوير الفوتوغرافي، يمكن أيضًا استخدامها في تنفيذ هجمات إرهابية، حيث تستطيع الطائرة من دون طيار أن تحمل سلاحًا موجهًا أو قنبلة أو عبوة ناسفة، وتفجيرها على الهدف المرصود، أو استخدامها في عمليات المُراقبة والاستطلاع، فالوسيلة واحدة، والاستخدام واحد، ويتبقى فقط الهدف من الاستخدام، سواء حمل طرد أو قنبلة.

وتمتلك الدرونز، أو الطائرات من دون طيار التجارية عديدًا من المميزات التي جعلتها جاذبة للحركات الإرهابية، فالشركات المنتجة لهذه الدرونز عندما طرحتها كان الهدف منها الاستخدام الشخصي أو التجاري، فكان تصميمها يتلاءم مع الهدف، وهو أن تكون صغيرة، وأن تكون تكلفتها أيضًا قليلة، وتكون

في متناول الأفراد، وقد بدأت الشركات المنتجة في التنافس، لتطوير إمكانيات هذه الطائرات مع تقديم سعر منافس في السوق، وإتاحتها للاستخدام من قبل الأفراد العاديين الذين لا يملكون أي مهارة خاصة لاستخدامها.

ولهذه الأسباب امتلكت هذه الطائرات ميزات جاذبة للحركات الإرهابية، مثل صعوبة رصدها من قبل الرادارات بسبب بنيتها الصغيرة، واستهلاكها المنخفض للطاقة، وقدرتها على قطع مئات الكيلو مترات، فضلًا عن إمكانياتها الفنية المتقدمة، وسعرها المنخفض، إذ تباع المروحيات الرباعية من طراز 2.0 (Parrot AR 2.0) بمبلغ 299 دولارًا أمريكيًّا، ويمكن التحكم بها عن طريق جهاز يعمل بنظام الأندرويد، وهو ما يفرض تحدِّيًا على الدول، إذ صار بإمكان أي جماعة إرهابية شراء طائرات درونز بتكلفة تقل عن تكلفة الآ ر بي جي، وقادرة على اختراق أغلب أنظمة الدفاعات البرية والهروب من أنظمة الردارات[1].

ولعل استخدام هذه الطائرات ليس بالأمر الجديد، ولكن الجديد هو تزايد الاعتماد عليها في القيام بعمليات إرهابية أو المساعدة في تنفيذها أو على الأقل تصويرها، حيث يشير عديد من التقارير إلى أن حزب الله يمتلك أسطولًا صغيرًا من الدرونز كمنصات أبابيل وميرساد الإيرانية ومنصات خاصة به. كما يشار إلى أن حزب الله استخدام تلك الطائرات في عام 2004 في التحليق في المجال الجوي الإسرائيلي، وبدأ من عام 2006 في إطلاق طائرات محملة بمواد متفجرة بهدف تفجير أهداف إسرائيلية. كما قام حزب الله أيضًا في عام 2012 باستخدام تلك الطائرات في مهام استطلاعية تتعلق بالمفاعل النووي الإسرائيلي. ولعل أول ضربة ناجحة لحزب الله باستخدام الطائرات من دون طيار كانت في نهاية عام 2014 حينما تمكن من قتل نحو 23 فردًا من الثوار السوريين[2].

1- تي. إكس. هامز، الدرونز نموذجًا: التوظيفات الإرهابية المُحتملة لـ"أنظمة التسليح المستقلة"، اتجاهات الأحداث، العدد 17، مركز المستقبل للأبحاث والدراسات المتقدمة، مايو يونيو 2016.

2- Hostile Drones: The Hostile Use Of Drones By Non-State Actors Against British Targets, Remotecontrolproject, January 2016, p 10-13 url: https://bit.ly/1mQ17BY

وفيما يتعلق بتنظيم"داعش"، يشير عديد من التقارير إلى امتلاكه طائرات من دون طيار واستخدامها في عمليات استطلاعية وتصويرية؛ وهذا ما ظهر في شريط فيديو بثه التنظيم يظهر فيه استخدام طائرات من دون طيار في عملية استطلاعية أثناء معركة مصفاة بيجي في العراق في عام 2015.

وفي نهاية سبتمبر 2016، هاجم تنظيم "داعش" بطائرة من دون طيار محشوة بالمتفجرات قوات تركية تنتشر في شمال سوريا، وفي 2 أكتوبر من العام نفسه قُتل اثنان من مقاتلي البيشمركة الأكراد في العراق وإصابة عنصرين من القوات الفرنسية الخاصة هناك بجروح بليغة نتيجة لانفجار طائرة بلا طيار.

إن هذا الاتجاه المتصاعد للاعتماد على الدرونز في القيام بعمليات إرهابية ازدادت وطأته خلال السنوات القليلة الماضية، من قبل الفاعلين العنيفين من دول الدول، بصورة تهدد أمن الدول بشكل حقيقي، خاصة تلك الدول التي لا تمتلك إمكانيات التشويش على هذه الطائرات أو اصطيادها في مجالها الجوي، كما أن الأمر لا يقتصر على استهداف القوات العسكرية فحسب، بل يمكن استهداف محطات الطاقة الرئيسية البعيدة من خلال الدرونز، أو حتى استهداف خطوط الطيران المدنية، حيث يمكن أن يتم استخدام الدرونز في تفجير إحدى طائرات الركاب المدنية، وذلك من خلال تعقبها على أحد برامج تعقب الطائرات المجانية، وتحديد خط سيرها، وتوجيه الدرونز المسيرة على نفس مسارها حاملة معها عبوة ناسفة يتم تفجيرها في حالة الاقتراب من الطائرة المدنية، خاصة إذا بدأت مرحلة الهبوط النهائي.

> يمثل الإرهاب السيبراني خطراً على الأمن القومي للدول في "مجتمع ما بعد المعلومات"، إذ يمكن من خلال توظيف التقنيات الذكية أن تقوم الجماعات الإرهابية وغيرها، بتنفيذ عمليات إرهابية سيبرانية، سواءً عبر هجمات إلكترونية في الفضاء الإلكتروني، أو استخدام الروبوت والدرونز في شن عمليات إرهابية، أو استخدام الطابعات ثلاثية الأبعاد في تصنيع الأسلحة، أو استخدام العملات الافتراضية لجلب التمويل غير المشروع.

ب- العُملات الافتراضية:

أصبحت البيتكوين العملة الرئيسية لجميع الأنشطة الإجرامية، لما لها من قدرات تشفيرية عالية، كما أنها لا تتطلب البيانات الشخصية للمستخدم، فأي مالك لعملة البيتكوين هو مجرد "رقم" يمثل المحفظة المالية التي سيتم تحويل النقود منها وإليها، وبالتالي فهي توفر خاصية التخفي وعدم التعقب.

وقد لجأت بعض التنظيمات المتطرفة لطلب تبرعات لها عبر الإنترنت بعملة البيتكوين، معلنة عن محفظة إلكترونية للتبرع من خلالها، للحصول على التمويل اللازم للعمليات الإرهابية، بل إنها تقوم أيضًا من خلال البيتكوين بشراء الأسلحة والمتفجرات والممنوعات من خلال المواقع الإلكترونية في الإنترنت الأسود، والذي يتم من خلاله تسويق هذه المنتجات بصورة غير شرعية.

ج- الطابعات ثُلاثيَّة الأبعاد:

تتعدَّد الاستخدامات الإيجابية للطابعات ثُلاثيَّة الأبعاد في مجال الطب، أو النقل، أو صناعة الأغذية، أو صناعة الفضاء، وغيرها من المجالات المختلفة، ومع ذلك فإن لها عديدًا من التهديدات الأمنية، مثل استخدامها في تصنيع الأسلحة والمخدرات، وتقليد المنتجات، وتزوير التحف والتماثيل، وسرقة حقوق الملكية الفكرية. وعلى الرغم من الأهمية المتزايدة لتوظيف الطابعات ثُلاثيَّة الأبعاد في مختلف الصناعات والمجالات، فإنه يمكن استخدامها أيضًا فيما يمكن اعتباره تهديدًا للأمن المُجتمعي، بل والأمن القومي للدولة، وذلك من خلال استخدامها في تصنيع الأسلحة من قبل أفراد عاديين أو من قبل جماعات إرهابية.

فطبقًا لتصريحات "مارك رولي" رئيس شرطة لندن والمفوض المساعد، فإن الإرهابيين من الممكن أن يستخدموا تلك التقنية في طباعة "طائرات من دون طيار" أو في صناعة القنابل أو بنادق ورصاص، ولمَّا كانت المواد المُستخدَمة في

تلك المواد من الصعب اكتشافها بواسطة الأجهزة الأمنية، فإن ذلك يعد مهددًا كبيرًا وتطورًا خطيرًا فيما يتعلق بالأنشطة الإرهابيية[1]، حيث يمكن للجماعات المتطرفة استخدمها في تنفيذ عملياتها الإرهابية سواء في تصنيع المتفجرات أو تهريبها عبر المطارات.

1-Sarah Anderson Goehrke, UK Police Note Potential for 3D Printing Uses in Terrorist Activity, 3dprint, accessed july 20, 2017 on: https://3dprint.com/59830/uk-anti-terror-3d-printing/

رابعًا: التهديدات غير التقليدية

هناك مصادر تهديد أخرى غير تقليدية وغير مباشرة أيضًا قد تتسبب في تهديد حالة الأمن في "ظل مُجتمع ما بعد المعلومات"، منها فقدان مصادر الطاقة على سبيل المثال أو الحرائق والكوارث الطبيعية، ففي هذه الحالة قد يتوقف المُجتمع عن العمل نتيجة تهديد مصادر الطاقة التي تعتمد عليها جميع التقنيات الذَّكيَّة. وذلك مثل:

1- فقدان مصادر الطاقة:

من مصادر التهديد غير المباشرة للأمن القومي للدُّول في ظل "مُجتمع ما بعد المعلومات" فقدان مصادر الطاقة الخاصة بالمدينة الذَّكيَّة أو المُجتمع الذكي، والذي يترتب عليه توقف كامل للخدمات التي تقدمها المدينة، وشلل في جميع الوظائف الحيوية التي يتم تقديمها داخل المدينة الذَّكيَّة، سواء كان هذا الفقد بفعل تخريبي مثل استهداف مباشر لمحطات الطاقة عبر تدميرها عن طريق التفجير أو الحرق أو الإتلاف، أو استهدافها عبر هجمات إلكترونية تؤدي أيضًا إلى نفس النتيجة، وهي خروج المحطة عن العمل وتوقف إمدادات الطاقة عن المدينة الذَّكيَّة.

2- التدمير المادي للخوادم:

يمكن إيقاف الخدمات في "مُجتمع ما بعد المعلومات" عبر استهداف الخوادم Servers التي تقوم بتقديم هذه الخدمات، سواء تم ذلك عبر تدميرها المادي بالإحراق أو الإتلاف، أو حتى قطع مصادر الطاقة عن المكيفات التي تعمل على تبريد هذه الخوادم؛ أو عبر هجمات إلكترونية تؤدي إلى إشغال الخوادم وعجزها عن أداء مهامها المطلوبة، أو حتى خروجها بصورة مؤقتة أو نهائية عن الخدمة.

3- الكوارث الطبيعية:

هي أحد أخطر أنواع مصادر تهديد الأمن القومي للدُّول، وهي تهديدات غير تقليدية، لا يتدخل فيها فاعل دولي بصورة رئيسية، مثل الزلازل، والبراكين، والتسونامي، والعواصف، التي يترتب عليها تدمير جميع أنواع البنية التحتية بالمدينة، سواء كانت تلك المدينة ذكية أو لا، وهذا التهديد يصعب مواجهته في كثير من الأحيان، وغالبًا ما يحتاج إلى إعادة إعمار كامل للمدينة بعد وقوع الكارثة.

الفصل الرَّابع

إعادة تعريف المفاهيم الأمنية في "مُجتمع ما بعد المعلومات"

حتى نهاية القرن العشرين كانت الموضوعات التي سادت في أدبيات الدراسات الأمنية هي القضايا التقليدية المتعلقة بالأبعاد العسكرية والاقتصادية، أما القضايا الجديدة التي ظهرت على الساحة، مثل الأمن الشخصي، والأمن البيئي، والأمن الصحي والأمن الثقافي، وبالطبع الأمن السيبراني؛ فمعظمها قضايا مستحدثة تندرج في نطاق الأمن غير التقليدي.

وتمثلت إحدى المحاولات الأولية والمهمة للتعبير عن تلك الحاجة في توسيع مفهوم الأمن بحيث لا يقتصر على التهديدات التقليدية، فيما أورده "ريتشارد أولمان" في مقاله المهم "إعادة تعريف الأمن"، الصادر في عام 1983 في مجلة International Security، فبحسب أولمان، فإن "المنظور الضيق للأمن القومي باعتباره يتلخص في حماية الدولة من هجمات عسكرية عبر الحدود خاطئ وخطر في آنٍ واحد"، ويوضح "أولمان" أن هذا المنظور الضيق يحول الاهتمام بعيدًا عن التهديدات غير العسكرية التي توقع أن تقوض استقرار عديد من الدول خلال السنوات المقبلة.

> آثار الذكاء تعيش أكثر من آثار القوة
>
> فرانسيس بيكون

كما حذر "أولمان" من افتراض هذا المنظور، ضمنًا، أن التهديدات التي تنبع من خارج حدود الدولة هي بشكل ما أكثر خطورة على أمنها من التهديدات التي قد تنشأ من داخلها، مقدمًا ما يمكن اعتباره التعريف الأكثر شمولًا للتهديدات غير التقليدية للأمن قائلًا: "إن التهديد للأمن القومي هو نشاط أو سلسلة أحداث تهدد بشكل كارثي، وخلال مدى زمني محدود نسبيًّا، بتدهور مستوى معيشة سكان دولة ما، أو تهدد بشكل جوهري، بتقليص مدى الخيارات السياسية المتاحة أمام حكومة تلك الدولة، أو وحدات خاصة غير حكومية داخلها، سواء أكانت هذه الواحدات أفرادًا، أم جماعات، أم مؤسسات".

كما طور "برنامج الأمم المتحدة الإنمائي" ما يمكن اعتباره تعريفًا إجرائيًّا لما اعتبره البرنامج تهديدات غير تقليدية للأمن في إطار مفهوم الأمن الإنساني، في محاولة لتفسير ظواهر جديدة من التهديد الأمني، وحدد أبرز خصائصها في أنها: ذات صبغة عالمية لا تقتصر على دولة ما، ومتداخلة، بحيث يمكن أن يفضي أحد التهديدات إلى تهديد آخر، أو يفاقم من تداعياته السلبية، ولا يمكن التعامل معها بشكل جذري، وفقًا لمقولات مفهوم الأمن في صياغته التقليدية.

وحدد التقرير سبعة أنماط من تلك التهديدات هي: (الأمن الاقتصادي، والأمن الغذائي، والأمن الصحي، والأمن البيئي، والأمن الشخصي، والأمن المُجتمعي، والأمن السياسي[1].

ويُعتبر "الأمن السيبراني" أحد عناصر الأمن القومي غير التقليدية، وذلك لأن أحد مستخدمي الفضاء الإلكتروني بإمكانه أن يُوقع خسائر فادحة بالطرف الآخر، وأن يتسبب في شل البينة المعلوماتية والاتصالاتية الخاصة به، وهو ما يسبب خسائر عسكرية واقتصادية فادحة، من خلال قطع أنظمة الاتصال بين الوحدات العسكرية وبعضها البعض، أو تضليل معلوماتها أو سرقة معلومات سرية

1- أ.د. محمد جمال مظلوم، الأمن غير التقليدي، جامعة نايف العربية للعلوم الأمنية، الرياض، 2012، ص 85.

عنها، أو من خلال التلاعب بالبيانات الاقتصادية والمالية وتزييفها أو مسحها من أجهزة الحواسب، أو السيطرة على نظم الذَّكاء الاصطناعي وإنترنت الأشياء، أو اختراق أسراب من الدرونز أو الرُّوبوتات أو السيارات ذاتية القيادة وتوجيهها للقيام بأعمال تخريبية.

وعلى الرغم من فداحة الخسائر، فإن الأسلحة بسيطة، فهي عبارة عن برمجيات لا تتعدى الكيلو بايتس، تمثل في فيروسات تخترق شبكة الحاسب الآلي وتنتشر بسرعة بين الأجهزة، وتبدأ عملها في سرية تامة وبكفاءة عالية، وهي في ذلك لا تفرق بين المقاتل والمدني، وبين العام والخاص، وبين السري والمعلوم.

وتتعدَّد تعريفات الأمن السيبراني، فهناك من يقوم بتوسيعها لكي تعبر عن القدرة على حماية بيانات الدولة وشبكاتها مثل تعريف Lewis, J. A بأنه "حماية شبكات الحاسوب والمعلومات التي تحتويها من الاختراق أو التدمير أو الاضطرابات الضارة[1]"، وهناك تعريف للأمن الإلكتروني يرى أنه "القدرة على حماية أو الدفاع عن استخدام الفضاء السيبراني من الهجمات السيبرانية[2]"، أو هو "فن ضمان وجود واستمرارية مُجتمع المعلومات في دولة ما، وضمان وحماية المعلومات والأصول والبنية التحتية الحيوية في الفضاء الإلكتروني[3]".

ومن التعريفات من يحدد إجراءات وسياسات للأمن السيبراني، مثل تعريف "الاتحاد الدولي للاتصالات"، الذي يشير إلى أنه "مجموع الأدوات والسياسات والمفاهيم الأمنية والضمانات والمبادئ ومناهج إدارة المخاطر والإجراءات

1-Lewis, J. A, Cybersecurity and Critical Infrastructure Protection, Center for Strategic and International Studies, . Washington, DC, 2006. Accessed March 9 2017 on http://csis.org/publication/cybersecurity-and-criticalinfrastructure-protection
2-Committee on National Security Systems, CNSSI No. 4009, April 6, 2015, P40, Accessed March 10, 2017, on: https://bit.ly/2T4dgnm
3-Canongia, C., & Mandarino, Cybersecurity: The New Challenge of the Information Society, Hershey, 2014 p 60.

والتدريبات وأفضل الممارسات والضمانات التكنولوجية التي يمكن استخدامها لحماية البيئة السيبرانية والمستخدم والمنظمة بصورة عامة[1]". كما يُعرف الأمن الإلكتروني أيضًا بأنه عملية "الحد من خطر الهجمات الضارة على برامج وأجهزة الكمبيوتر والشبكات، من خلال استخدام أدوات كشف الاختراقات، ووقف نشاط الفيروسات، ومنع الدخول غير المصرح به، وتأكيد الهويات، وتمكين الاتصالات المشفرة[2]"، وهو أيضًا "مجموعة من التقنيات والعمليات والممارسات والاستجابات وتدابير الحد من المخاطر المصممة لحماية الشبكات والحواسيب والبرامج والبيانات من الهجوم أو الضرر أو الوصول غير المصرح به من أجل ضمان السرية والنزاهة والاتاحة[3]"،

إن أحد التحديات الصعبة التي تثيرها التطورات التكنولوجية الجديدة، تتمثل في قدرة الحكومات على التكيف مع حاجات المواطنين، وكيفية استجابتها وتعاملها مع التدفق الهائل للمعلومات، وتقديمها خدمات أكثر ذكاءً وسرعة، والأهم قدرتها على التعامل مع مجتمعات لم ولن تُعد مغلقة، علاوة على آليات الاستجابة للمخاطر الأمنية المختلفة الناتجة عن مخرجات الذكاء الاصطناعي والمحركات الأخرى للثورة الصناعية الرابعة.

كما تعرفه أيضًا وزارة الداخلية الأمريكية بأنه "النشاط أو العملية، القدرة أو الإمكانية، أو الحالة التي يمكن من خلالها حماية المعلومات ونظم الاتصالات والدفاع عنها من الضرر أو التعديل أو التجسس أو التدمير أو الدخول غير المصرح به[4]".

1- Cybersecurity Guide for Developing Countries, ITU, 2009. Accessed March 10, 2017 on: https://bit.ly/2rQ5Rfy

2 -Dan Craigen, Nadia Diakun-Thibault, and Randy Purse, Defining Cybersecurity, Technology Innovation Management Review, October 2014, p15. Accessed March 9 2017, on: https://bit.ly/2QM4my9

3- Canada's Cyber Security Strategy, Government of Canada, Ottawa 2010, Accessed March 10, 2017 on: https://bit.ly/2nmfAXL

4- A Glossary of Common Cybersecurity Terminology, National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security, (DHS), accessed March 11, 2017 on http://niccs.us-cert.gov/glossary#letter_c

وبالتالي، فقد ساهمت الابتكارات التكنولوجية الحديثة وتبني نماذج الحكومات الذَّكيَّة والمدن الذَّكيَّة وتزايد الاعتماد على التقنيات المتطورة في إدارة جميع شؤون الحياة اليومية في تغير المفاهيم التقليدية للعلاقات الدولية، خاصة تلك المرتبطة بالأمن القومي، مثل القوة، والحرب، والصراع، والردع، والدفاع. ومن هنا ظهرت الحاجة إلى تطوير استراتيجيات جديدة، تتلاءم مع العصر السيبري Cyber Age... ذلك العصر الذي يعتبر الإنترنت فيه هو الإطار العام الحاكم لجميع تفاعلاته، سواء كانت شخصية أو عامة، عسكرية أو سياسية، اقتصادية أو اجتماعية، فتم إعادة تعريف مفهوم الحرب ليظهر شقها السيبراني، وظهر شكل جديد من أشكال القوة هو القوة السيبرانية، وتمت إعادة صياغة مفهوم الردع ليشمل الردع السيبراني Cyber Deterrence باعتباره إحدى الأدوات الرئيسية في منظومة التوازن الاستراتيجي، وهو ما يحاول هذا الفصل التعرض له.

أولًا: مفهوم القوة السيبرانية

تتعدَّد أدوات ممارسة القوة في العلاقات الدولية وفقًا لقدرات وإمكانيات ورغبات القوى المشاركة فيها، فقد تكون القوة العسكرية من أهم هذه الأدوات، وقد تكون القوة الاقتصادية والحصار الاقتصادي والمالي العامل الرئيسي للسيطرة على الخصم وممارسة القوة عليه، وقد تكون الأداة المعلوماتية من خلال وسائل الاتصال والتكنولوجيا الحديثة والإنترنت هي العامل الرئيسي لحسم صراع بين دولتين.

ولكن ممارسة القوة والنفوذ قد تطورت بشكل هائل نتيجة للتطور الكبير في المعلومات، مما جعل هذه المعلومات هي الهدف الأساسي الذي تسعى الدول للحصول عليه، فثمة معلومات مكنت الدول من نتاج السلاح النووي، وظل هذا التطور مستمرًّا، حيث اعتمدت كل مرحلة من مراحل التطور الإنساني على سلطة أو قوة من طبيعة معينة تتناسب مع متطلبات هذه المرحلة. وقد أثرت هذه السلطة أو القوة بصورة مباشرة أو غير مباشرة في أدوات الصراع بين المُجتمعات وآلياتها، وأفرزت مفردات ومكونات تكاملت معًا لتنتج نظامًا دوليًّا سيطرت مفاهيمه بعض الوقت أو كل الوقت.

وفي هذا الإطار، يتميز العصر الراهن بظاهرة الثَّورة العلمية والتكنولوجية، حيث أزاحت التكنولوجيا كثيرًا من عناصر القوة عن مواقعها التي تربعت عليها لفترة طويلة، مما عرض المفهوم التقليدي للقوة إلى انتقادات، وأفصح عن محتوى جديد للقوة، فلم يعد ما لدى الدولة من قدرات عسكرية أو ما تمتلكه من أموال وثروات، عناصر كافية لبلورة دورها كقوة مؤثرة وفاعلة[1].

1- عادل عبد الصادق، الإرهاب الإلكتروني: القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة، مركز الأهرام للدراسات السياسية والاستراتيجية، القاهرة، 2009 ص 50 - 58.

وأصبح من الأمور المستقرة في العلاقات الدولية أن مصادر قوة الدولة وأشكالها تتغير، فإلى جانب القوة الصلبةHard Power التي تتمثل في القدرات العسكرية والاقتصادية، تزايد الاهتمام بالأبعاد غير المادية للقوة، ومن ثم برز دور القوة الناعمة Soft power التي تعتمد على جاذبية النموذج والإقناع، ومع ثورة المعلومات والقدرة على إنتاج التكنولوجيا المتطورة عن طريق الاختراع والإبداع، ظهر شكل جديد من أشكال القوة هو القوة السيبرانيةCyber Pow-er، والتي تصاعد تأثير على المستويين الدولي والمحلي، فمن ناحية أدت إلى توزيع وانتشار القوة بين عدد أكبر من الفاعلين؛ مما جعل قدرة الدولة على السيطرة على هذا الميدان موضع شك، مقارنة بالمجالات الأخرى للقوة. ومن ناحية أخرى جعلت القوة الإلكترونية بعض الفاعلين الأصغر في الساحة العالمية لديهم قدرة أكبر على ممارسة كل من القوة الصلبة والقوة الناعمة عبر الفضاء الإلكتروني، وهو ما يعني تغيرًا في علاقات القوى في السياسات الدولية[1].

ويُعتبر أستاذ العلاقات الدولية الشهير "جوزيف ناي" من أهم من تحدثوا عن القوة الإلكترونية كشكل جديد للقوة، حيث يعرفها "ناي" بأنها "القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء الإلكتروني، أي أنها القدرة على استخدام الفضاء الإلكتروني لخلق مزايا، والتأثير في الأحداث المتعلقة بالبيئات الواقعية الأخرى، وذلك عبر أدوات إلكترونية"[2]. ويعرفها "دانيال كويل Daniel T. Kuehl" بأنها "القدرة على استخدام الإنترنت لخلق مزايا والتأثير على الأحداث في البيئات التشغيلية جميع من خلال أدوات القوة"[3].

1- د. سعاد محمود أبو ليلة «دورة القوة: ديناميكيات الانتقال من (الصلبة) إلى (الناعمة) إلى (الافتراضية)»، مجلة السياسة الدولية، ملحق اتجاهات نظرية: القوة: كيف يمكن فهم تحولات القوة في السياسة الدولية؟، العدد 188 (أبريل، 2012)، ص 16.

2- Joseph S. Nye, Cyber Power, Op Cit. p4.

3- Daniel T. Kuehl, "From Cyber Space to Cyber Power: Defining the problems", in Franklin D. Krammer, Stuart Starr, and Larry K. Wentz. Eds, cyber power and national security, (Washington, D.C: National defense up, 2009(, p 16.

ويرى "جوزيف ناي" أن القوة الإلكترونية ترتبط بامتلاك المعرفة التكنولوجية، والقدرة على استخدامها. وهي تعني القدرة على استخدام الفضاء الإلكتروني في خلق مميزات والتأثير في الأحداث التي تجري عبر البيئات التشغيلية Op-erational Environments وعبر أشكال وأدوات القوة المختلفة، سواء كانت عسكرية، أو اقتصادية، أو دبلوماسية، أو معلوماتية[1].

وحدد "ناي" ثلاثة أنواع من الفاعلين الذين يمتلكون القوة الإلكترونية، يتمثل النوع الأول في الدولة، والنوع الثاني في الفاعلين من غير الدول، والنوع الثالث هم الأفراد. ويجادل "ناي" بأن مفهوم القوة السيبرانية يشير إلى "مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الإلكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه الوسائل"[2].

ويتضمن مفهوم القوة السيبرانية تغطية جميع القضايا التي تتعلق بالتفاعلات الدولية، والتي تشمل القضايا العسكرية والاقتصادية والسياسية والثقافية والإعلامية وغيرها، وهي تختلف عن مسمى "الحرب السيبرانية" التي تقتصر على التَّطبيقات العسكرية للفضاء الإلكتروني.

ويعتقد "جوزيف ناي" أيضًا أن هذه الفترة ليست الأولى التي يتأثر مفهوم القوة فيها بالتطور التكنولوجي، فقد تأثر العالم في القرن الخامس عشر باختراع الطباعة وما أحدثه من تطور في الإصلاح داخل أوروبا من خلال سهولة وصولها إلى الناس واستخدامها.

ويضيف أن الثَّورة التكنولوجية الحالية في بعض الأحيان تتم تسميتها بالثَّورة الصِّناعيَّة الثالثة التي تعتمد على صناعة متطورة وسريعة لأجهزة الكمبيوتر

1- Franklin D. Kramer, Stuart H. Starr, Larry Wentz,eds, Op. Cit, p 48.
2- Joseph S. Nye, Cyber Power, Op. Cit, P3

والاتصالات ونظم المعلومات والبرامج الحاسبية، والتي أثرت بصورة دراماتيكية على صناعة وخلق ونقل المعلومات[1].

ويرى "ناي" أن الدولة سوف تظل هي الفاعل المهيمن على الفضاء الإلكتروني، ولكن هناك فواعل أخرى سوف تشاركها في هذا الفضاء الإلكتروني، وسوف تجد الدُّول صعوبة في السيطرة عليه، فالحكومات قلقة من حالة تسرب المعلومات وتدفقها وصعوبة السيطرة عليها.

أصبح "الأمن السيبراني" أحد عناصر الأمن القومي غير التقليدية للدول، خاصةً وأن الأسلحة السيبرانية لا تفرق غالبًا بين ما هو مدني وعسكري، وبين ما هو عام وخاص، وبين ما هو مُعلن وسري. ولذلك تتوسع تعريفات "الأمن السيبراني"، بدءًا من حماية معلومات الدولة وشبكاتها من الاختراق، مرورًا بالقدرة على حماية الفضاء السيبراني من التعرض للهجمات، وصولًا إلى كونه فن ضمان وجود واستمرارية مجتمع المعلومات في الدولة وحماية بنيتها التحتية الحيوية ونظم الاتصال والدفاع عنها من الضرر أو التعديل من أطراف أخرى أو التجسس أو التدمير أو حتى مجرد الدخول غير المصرح به.

ويرى أيضًا أن القوى الكبرى ليست لها المساحة نفسها التي يمكن من خلالها السيطرة على الفضاء الإلكتروني مقارنة بقدرتها على السيطرة على الإقليم البحري أو البري، وأن الكيانات الافتراضية التي تنشأ عبر الإنترنت تستطيع أن تلتقي في إقليم افتراضي جديد خاص بها عبر الإنترنت وتؤسس لذاتها كيانات تنظيمية، ومن ثم يتراجع دور الدولة المركزية في حياة البشر. ويضيف أن الدول الكبرى التي تمتلك القوة الصلبة أو الناعمة، حتى الولايات المتحدة الأمريكية، وجدت نفسها تواجه مشاكل في السيطرة على حدودها على الإنترنت.

1-Ibid 1-3

ويؤكد "ناي" أن الفضاء الإلكتروني لن يزيل سيادة الدولة أو حدودها الجغرافية، ولكنه سوف يؤثر على مفاهيم القوة وتحولات القوة وأدواتها. **وقد حدد "ناي" أنماطًا لاستخدام القوة الإلكترونية، وميز بين الاستخدام الناعم لها والاستخدام الصلب، ويتضح ذلك في التالي:**

1- قدرة الفاعل (أ) على التأثير في سلوكيات الفاعل (ب)، ودفعه للقيام بأعمال لم يكن ليقوم بها، وتكون القوة الإلكترونية في هذه الحالة مصدرًا للقوة الناعمة كما في حالة اتجاه الدولة لوضع معايير ملزمة للبرمجيات، أو استخدام الجماعات الإرهابية للفضاء الإلكتروني في تجنيد بعض الشباب، بينما يكون استخدام القوة الإلكترونية بطريقة استخدام القوة الصلبة ذاتها من خلال الحرمان من خدمة الإنترنت، أو قطع خدمات الإنترنت عن الدولة كاملة.

فعلى سبيل المثال تعرضت إستونيا في عام 2007 لهجمات افتراضية، استهدفت بنيتها المعلوماتية. كما تم استخدام القوة الإلكترونية لاستهداف القوة الصلبة لدول أخرى، من خلال نشر فيروسات تدمر أجهزة الدولة، وتستهدف نظم الكمبيوتر الخاصة بالخدمات الحكومية[1].

2- قدرة الفاعل الدولي على التحكم في أجندة الآخرين من خلال إقصاء بعض استراتيجياتهم، وذلك من خلال أن يقوم الفاعل (أ) بمنع تنفيذ أجندة الفاعل (ب) من خلال العمل على إقصاء بعض استراتيجياته، ويتضح استخدام الفضاء الإلكتروني في ممارسة القوة الصلبة في هذا الوجه على سبيل المثال، في حالة منع الحكومة الإيرانية في عام 2010 - في أعقاب الاحتفال بعيد الثَّورة الإيرانية - بعض الناشطين السياسيين من عرض فيديوهات على موقع اليوتيوب مضادة للنظام الحاكم، حيث عمدت الحكومة إلى إبطاء سرعة الإنترنت وإعاقة بث هذه الفيديوهات، وبالتالي عملت على إقصاء إحدى استراتيجيات المعارضة الإيرانية في التعبير عن آرائها.

1- Joseph s.Nye, The Future of Power, speech before Pacific Forum, March 2011.

ومن مظاهر استخدام الفضاء الإلكتروني لممارسة القوة الناعمة بعض الشروط التي تضعها منظمة "الأيكان" على أسماء نطاقات الإنترنت، وكذلك المعايير الموضوعة، والتي لاقت قبولًا واسعًا لتصميم واستخدام البرمجيات[1].

3- ترتيب أولويات الفواعل الأخرى، وذلك من خلال قيام الفاعل (أ) بترتيب أولويات الفاعل (ب). ومن أمثلة ممارسة القوة الصلبة قيام بعض الدول، مثل الصين، والسعودية، بحجب بعض المواقع ونزع شرعيتها لدى المواطنين وترك مواقع أخرى مفتوحة لهم، وكذلك قيام الولايات المتحدة الأمريكية باتخاذ عدة إجراءات ضد شركات بطاقات الائتمان لمنع ممارسة القمار عبر الإنترنت. ومن أمثلة القوة الناعمة العمل على نشر أو تقييد قيم وثقافات عبر الإنترنت، مثل تطوير قيم رافضة لنشر الإباحية عبر الإنترنت[2].

وبالتالي أصبحت القوة الإلكترونية حقيقة أساسية في العالم بكل مظاهرها المتنوعة، بما عمل على دعم ومساندة العمليات الحربية والاقتصادية والسياسية، وبروز مُجتمع المعلومات الدولي والاقتصاد الإلكتروني الجديد الذي أثر على طبيعة النظام الدولي، والعمل على توزيع الموارد الاقتصادية ومستويات النمو الاقتصادي وأنماط التفاعل بين القوى الاقتصادية الدولية، والتأثير على القوة السياسية من خلال المشاركة المقصودة في عمليات صنع القرار في النظام الدولي[3].

1- Joseph S. Nye, Cyber Power, Op. Cit, p 7 -9

2-Ibid, p 9

3- عادل عبد الصادق «مصر ومجتمع المعلومات: هل يمكن تكرار التجربة الهندية؟»، مجلة أحوال مصرية، العدد 17، (مركز الدراسات السياسية والاستراتيجية بالأهرام، يوليو 2004).

ثانيًا: مفهوم الحرب السيبرانية

على الرغم من أن الحديث عن الحرب السيبرانية يعود لما يقرب من ربع قرن من الزمان، فإن هذا المفهوم لا يزال يشهد حالة من الغموض وعدم الوضوح، بل وعدم اتفاق بين الأكاديميين أيضًا حول ما إذا كانت الحرب السيبرانية حقيقة أم لا، وأن سببها الرئيسي التطور المتسارع في التقنيات الذَّكيَّة وتزايد الاعتماد على التكنولوجية في الحياة اليومية، وضيق الفجوة بين التقنيات الميدانية والعسكرية في الفضاء الإلكتروني، مما جعل الظاهرة – أي ظاهرة الحروب السيبرانية - تتشكل ويُعاد تشكيلها بصورة مستمرة، وهو ما أدى إلى عدم صقل المفهوم واتضاح جميع أبعاده بصورة كاملة، على الأقل لدى المُجتمع الأكاديمي، حتى أصبح هناك مفهومان للحرب السيبرانية هما:Cyber War & Cyber Warfare.

وفي محاولة للتمييز بينهما، أجرى كلٌّ من Andrew Colarik and Daniel Hughes دراسة في الخطاب السياسي والعسكري صادرة في عام 2017 بعنوان "The Hierarchy of Cyber War Definitions"، وتوصلا إلى أنه بينما يقصد بالأولى أي Cyber War تصرف الحرب ذاته، فإنه يقصد بالثانية Cyber Warfare الوسائل اللازمة لإدارة هذه الحرب[1].

وكانت أولى الكتابات التي تنبَّأت بالحرب السيبرانية لكل من John Arquilla And David Ronfeldt، وذلك في مقالهما المنشور عام 1993 بعنوان Cyber-war Is Coming[2] حينما حذَّرا من أن الحرب السيبرانية مقبلة. وعرف الكاتبان الحرب السيبرانية بأنها "تنفيذ، والاستعداد لتنفيذ، العمليات العسكرية وفقًا للمبادئ المعلوماتية، من خلال تعطيل –إن لم يكن تدمير - نظم المعلومات

1- Andrew Colarik and Daniel Hughes, The Hierarchy of Cyber War Definitions, Massey University, Palmerston North, New Zealand, Springer International Publishing AG, 2017, p 17.
2- John Arquilla, David Ronfeldt, Cyberwar is Coming!, 1993, Published online On Jan 1, 1997, Accessed December 5, 2017, on: https://www.rand.org/pubs/reprints/RP223.html

والاتصالات على أوسع نطاق"، بل إن الكاتبين وسعا مفهوم الحرب السيبرانية ليشمل أيضًا أبعادًا غير مادية تتمثل في "تدمير العقيدة العسكرية للعدو، والتي تمثل الأساس الذي يعتمد عليه لتحديد هويته وخططه وتصرفاته وأهدافه والتحديات التي يواجهها"، وذلك عبر معرفة كل شيء عن العدو ومنعه في الوقت نفسه من معرفة أي شيء عن الطرف الآخر، وتحويل ميزان المعرفة ليكون في صالح هذا الطرف، فالحرب السيبرانية هي عملية "توظيف المعرفة بهدف الاقتصاد في توظيف رأس المال والعمالة"، أو حتى في حالة عدم تكافؤهما مع الخصم[1].

ويعرفها "جوزيف ناي" بأنها الأعمال العدائية في الفضاء السيبراني، التي لها آثار تعادل أو تفوق العنف الحركي التقليدي[2]، في حين يعرفها كينيث جريس Kenneth Geers بأنها "القدرة على الدفاع عن والهجوم على المعلومات، من خلال شبكات الحاسب الآلي عبر الفضاء الإلكتروني، بالإضافة إلى شل قدرة الخصم على القيام بنفس هذه الهجمات"، وتشمل الحرب السيبرانية عند "جريس" خمسة عناصر رئيسية هي: (التجسس، والدعاية، والحرمان من خدمة الإنترنت، وتعديل البيانات والتلاعب بها، وتعطيل البنى التحتية الحيوية[3].

وإذا كان كلٌّ من John Arquilla, David Ronfeldt, and Richard Stien-non قد أكدوا أن الحرب السيبرانية مقبلة لا محالة، فإن توماس ريد Thomas Rid في مقاله الصادر عام 2011 بعنوان Cyber War Will Not Take Place يجزم بأن الحرب السيبرانية لم تحدث في الماضي، ولا تحدث حاليًا، ولن تحدث

1- John Arquilla, David Ronfeldt, Cyberwar is Coming!, In Athena's Camp: Preparing for Conflict in the Information Age, RAND Corporation, 1997, P30.

2-Nye, Jr., Joseph S. 2011. Nuclear Lessons for Cyber Security? Strategic Studies Quarterly, 5(4): 18-38, accessed December 5, 2017, on https://dash.harvard.edu/bitstream/handle/1/8052146/nye-nuclearlessons.pdf?sequence=1

3- Kenneth Geers, Cyber Space and the changing nature of warfare,(U.S. Representative Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia). On : http://www.carlisle.army.mil/DIME/CyberSpace.cfm On August15, 2013

في المستقبل، وذلك عبر تعريف الحرب السيبرانية بأنها "ممارسة النفوذ عبر توظيف البرمجيات الخبيثة بصورة سياسية ووظيفية وقاتلة"، ومن خلال تفنيد الأحداث التي شهدت توظيف القوة السيبرانية، يرى "ريد" أن الأمر لا يتعدى كونه "هجمات سيبرانية Cyber Attacks" وليس حربًا سيبرانية، وأن الهجمة السيبرانية تسعى بالأساس لتحقيق ثلاث وظائف رئيسية أقدم من فكرة الحرب نفسها، وهي التخريب، والتجسس، والتدمير[1].

اتجهت العديد من الدول إلى تأسيس ما يُسمى "الجيوش السيبرانية"، والتي تتمثل مهماتها الرئيسية في: مهاجمة شبكات الخصم، واستطلاعها والتجسس عليها، والدفاع عن شبكات الدولة. والأكثر من ذلك أن محترفي القرصنة المدنيين أضحوا عنصرًا مهمًا باعتبارهم "جنود ظل" في صفوف القوات المسلحة التقليدية، بما لديهم من إمكانيات وتقنيات برمجية وإلكترونية تمكنهم من تغيير قواعد اللعبة في أوقات الأزمات والحروب.

وعلى النقيض يرى كل من Richard Clarke And Robert Knake في كتابهما الصادر بعنوان (الحرب السيبرانية: الخطر القادم على الأمن القومي وكيفية التعامل معه) Cyber War :The Next Threat to National Security and What to Do About It أن الحرب السيبرانية قد بدأت بالفعل، وأنها حرب حقيقية، تحدث بسرعة الضوء، وعلى نطاق عالمي، وتتخطى ساحة المعركة[2].

وقد اتَّجه عديد من الدول إلى تجنيد محترفي القرصنة والبرمجة في صفوف القوات المسلحة التقليدية، وأصبحوا يشكلون ذراعًا أساسيَّة للمساهمة في تحقيق أهداف الدولة، وباتوا بمثابة "جنود ظل" يعملون خلف شاشات

1- Thomas Rid, Cyber War Will Not Take Place, Journal of Strategic Studies, Volume 35, 2012, Pages 5-32, Published online: 05 Oct 2011, on http://www.tandfonline.com/doi/abs/10.1080/01402390.2011.608939

2- Richard A. Clarke And Robert K.Knake, Cyber War: The Next Threatto National Security and What to DoAbout It, harpercollins, 2010, p18

الكمبيوتر، ولديهم من الإمكانيات والتقنيات البرمجية والإلكترونية ما يمكنهم من تغيير قواعد اللعبة في أوقات الأزمات والحروب، فأصبحوا هم عماد إدارة الصراعات العسكرية.

ويمكن تصنيف المهام التي يمكن أن تقوم بها الجيوش السيبرانية في ثلاثة أنواع رئيسية، هي مهاجمة شبكات الخصم، واستطلاعها والتجسس عليها، والدفاع عن شبكات الدولة، **ويتضح ذلك في التالي:**

1- مهاجمة الشبكات Computer Network Attack :

تشمل اختراق الشبكات لحقن الحاسبات بكمٍّ هائل من البيانات لتعطي لها أو وضع بيانات ومعلومات محرفة لإرباك مستخدمي الحاسبات، ونشر الفيروسات وما شابهها من البرامج الصغيرة المؤذية مثل الديدان، وتلغيمها بالقنابل المنطقية التي يتم تنشيطها في الوقت المناسب للمهاجم لكي تتلف ما تحتويه الحاسبات من بيانات وبرمجيات، أو القيام بهجمات سيبرانية أو مادية لقطع لخدمات الإنترنت عن الخصم، وتدمير قواعد البيانات التي يمتلكها، وتعطيل قدرته على النشر السريع لقدراته وإمكانياته وقواته، أو قطع أنظمة الاتصال بين الوحدات العسكرية وبعضها وتعطيل شبكات الكمبيوتر، أو شل أنظمة الدفاع الجوي أو التوجيه الإلكتروني للخصم، أو السيطرة على وحدات القيادة والتوجيه، أو فقدان العدو قدرته على التحكم أو الاتصال بالأقمار الصِّناعيَّة[1].

وقد يصل الأمر إلى التدمير الفعلي (Physical Destruction) من خلال تدمير الجانب المادي، مثل الخادمات، والأسلاك، والكابلات، والأجهزة التي تحتوي على معلومات يصعب التأثير عليها من بعد، وتتم عملية التدمير بالأسلحة التقليدية كالجوية والبحرية والبرية أو بعمليات القوات الخاصة.

1- Colonel Jayson M. Spade, China’s Cyber Power And America’s National Security, Jeffrey L. Caton Editor, (U.S. Army War College, May2012) p 7

2- الدفاع عن الشبكات Computer Network Defense:

تشمل هذه العملية حماية الشبكات وأجهزة الكمبيوتر من أي عملية اختراق خارجي، ويجب أن يكون التأمين على مستوى البرمجيات (Software) والمكون المادي للشبكات (Hardware)، بحيث يتم تأمين الشبكة من أي اختراق خارجي بأي من الأسلحة السيبرانية السابق ذكرها، وكذلك تأمين المكون المادي للشبكات مثل الخوادم أو الشَّرائح الإلكترونية، والتي قد تكون مبرمجة من قبل المصمم لكي تعمل في ظروف غير عادية لصالحه[1].

3- استطلاع الشبكات Computer Network Exploitation:

تعني القدرة على الدخول غير المشروع والتجسس على شبكات الخصم، دون أن يصاحب ذلك تدمير أو تخريب للبيانات والمعلومات، بهدف الحصول على هذه المعلومات، والتي قد تشمل خطط دفاع وهجوم عسكري، أو أسرارًا عسكرية وحربية، أو معلومات سياسية واستخباراتية، ولا تتوقف وظيفتها على ذلك فحسب، بل يمكن من خلالها عمل خرائط لشبكات الحاسب الآلي واستخدامها مستقبلًا في عمليات الهجوم الإلكتروني، كما يمكن ترك بعض الثغرات من خلال الأبواب الخلفية (Backdoors) لحقن الشبكة بفيروسات للقيام بمهام معينة مثل نقل البيانات إلى أجهزة المتجسس[2]، كما يمكن أيضًا استخدامها في التأثير على أفكار وسلوكيات الخصم من خلال شن حرب نفسية، وذلك بنشر مثل هذه الخطط العسكرية والبيانات أو إرسالها إليه مرَّة أخرى لكي يدرك إلى أي مدى هو مُخترق ولن يستطيع المواجهة.

1-Ibid, 9

2-Dennis M. Murphy, ed., Information Operations Primer, (Carlisle, Pennsylvania: U.S. Army War College, 2010), p 169

ووفقًا لما سبق، فإن عديدًا من دول العالم اتَّجهت في السنوات الأخيرة إلى تأسيس قوى سيبرانية رئيسية، أي لديها وحدات قتالية خاصة بالحرب السيبرانية، وتتميز بقدراتها الهجومية والدفاعية المتقدمة، ومن أبرز هذه الدول: الولايات المتحدة الأمريكية، والصين، وروسيا، وإسرائيل، حيث:

1- القيادة السيبرانية الأمريكية (US Cyber Command):

استحدث البنتاجون في يونيو 2009 قيادة عسكرية مهمتها الرد على هجمات قراصنة المعلومات وتنفيذ عمليات في الفضاء الإلكتروني[1]. وقد تم تعيين أول جنرال عسكري لإدارة حروب الفضاء الإلكتروني، وهو الجنرال ألكسندر كيث.

وتستهدف وزارة الدفاع الأمريكية من تلك القيادة الجديدة أن تشرف على مختلف الجهود المتعلقة بالإنترنت في كل أجهزة القوات المسلحة، سواء من حيث تأمينها أو القيام بعمليات سيبرانية عسكرية ضد أهداف خارجية. وقد وصل عدد قوات القيادة العسكرية للفضاء الإلكتروني إلى 6000 مقاتل بحلول عام 2016[2].

وقبل استحداث هذه القيادة كانت الحكومة الأمريكية تعتمد على وكالة المخابرات المركزية (CIA)، ووكالة الأمن القومي الأمريكي (NSA) للقيام بعملياتها في الفضاء الإلكتروني، بل إن معظم مشاريع التجسس الإلكتروني الكبرى للولايات المتحدة مثل بريزم (PRISM) وغيره، نفذتها وكالة الأمن القومي.

1- عادل عبد الصادق، أمريكا وتشكيل قيادة عسكرية في الفضاء الإلكتروني.. هل بدأ الاستعداد لحروب المستقبل؟، مجلة أحوال مصرية، عدد 130، (مركز الأهرام للدراسات السياسية والاستراتيجية، يوليو 2009)، يمكن المطالعة على: https://bit.ly/2GLnbwx

2- U.S. cyberwarfare force to grow significantly, defense secretary says, Washington Post, Accessed Nov 15, 2014: https://wapo.st/1hHdTsH

وتتمثل المهمة الرئيسية لهذه القيادة في حماية شبكات وزارة الدفاع وأنظمتها، والاستعداد لخوض حروب الفضاء الإلكتروني والدفاع عن شبكات الدولة الأمريكية، من خلال إدارة عمليات شبكات المعلومات التابعة لوزارة الدفاع الأمريكي، لتحقيق هدفين رئيسيين هما: حماية حرية عمل الولايات المتحدة وحرية عمل حلفائها في الفضاء الإلكتروني، وحرمان أعداء الولايات المتحدة – عند الحاجة – من حرية العمل في الفضاء الإلكتروني.

2- الوحدة 61398 في الصين:

هي وحدة تتسم بأنشطتها السرية داخل جيش التحرير الشعبي الصيني، حيث تقوم بعمليات التجسس الإلكتروني، وسرقة المعلومات الاقتصادية، خاصة من الولايات المتحدة الأمريكية. وقد أكد تقرير صادر في فبراير 2013 عن شركة "مانديات" الخاصة بالأمن الإلكتروني، أن الوحدة 61398 بدأت في شن أولى هجماتها منذ عام 2006، وقامت بسرقة مئات التيرابيتس Terabytes من البيانات الخاصة بـ141 منظمة تشمل المخططات التكنولوجية، وعمليات التصنيع والبيانات والوثائق وخطط التسعير والتسويق، ورسائل البريد الإلكتروني وقوائم الاتصال. ولُوحِظَ أن ما لا يقل عن 115 شركة من هذه الشركات تقع في الولايات المتحدة الأمريكية[1].

ويُعتقد أن الوحدة 61398 تخضع لإدارة المكتب الثاني التابع للإدارة الثالثة لهيئة أركان جيش التحرير الشعبي، وتقع في منطقة شنغهاي، وتقوم شركة الاتصالات الصينية بإمدادها بنوع خاص من الألياف الضوئية لنقل بيانات الإنترنت، ويعتقد التقرير أن الوحدة تضم أو أنها هي نفسها تشكل ما أطلقت عليه شركة "مانديت" اسم التهديد المقبل المستمر Advanced Persistent

1- APT1, Exposing One of China's Cyber Espionage Units, Mandiat Report, 2013: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Threat، وهي الوحدة التي قامت بالهجوم على عدد كبير من المؤسسات الصِّناعيَّة والحكومية حول العالم منذ عام 2006 على الأقل. وتعتمد الوحدة 61398 على شبكة من القراصنة الإلكترونيين الصينيين في 13 دولة، يقع معظمها في الولايات المتحدة التي بها أكثر من 100 جهاز كمبيوتر مخصص لغرض العمليات السيبرانية.

وفي 19 مايو 2014، ولأول مرَّة في التاريخ، وجَّه المدعي العام الأمريكي إريك هولدر – باسم مكتب التحقيقات الفدرالي – تهمًا جنائية بسرقة معلومات تجارية حساسة من خمس شركات أمريكية كبرى (أبرزها يو إس ستيل، وألكوا، وستنجهاوس للإلكترونيات، وسولار وورلد)، إلى خمسة ضباط في الوحدة 61398 التابعة للجيش الصيني، وطلب من الحكومة الصينية تسليمهم للولايات المتحدة[1]، ودائمًا ما تواجه الصين الاتهامات الموجهة إليها بالقيام بهجمات سيبرانية أو سرقة معلومات سرية بالنفي، والادعاء بأنها أيضًا ضحية لعمليات قرصنة إلكترونية.

3- قراصنة الظل التابعين للحكومة الروسية:

صرَّح المتحدث باسم وزارة الدفاع الروسية "إيجور يجوروف" في أكتوبر 2014، بأن روسيا تخطط لبناء نظام إلكتروني شامل على مراحل بحيث يتم الانتهاء منه في عام 2017، وذلك بهدف حماية البنية الأساسية للقوات المسلحة من الهجمات السيبرانية. كما أمر وزير الدفاع "سيرجي شويجو" في عام 2014 أيضًا بأدراج 500 من الطلبة المتميزين في استخدام الحاسب الآلي في "وحدات علمية" خاصة، وسيعتبر عملهم مثل الخدمة العسكرية[2].

1- 5 in China Army Face U.S. Charges of Cyberattacks, The New York times, Accessed Nov 15, 2014https://nyti.ms/1hXAxhg

2- روسيا تنشئ وحدات إلكترونية في قوات الصواريخ الاستراتيجية، خبر منشور على وكالة أنباء شينخو الصينية، بتاريخ مطالعة 11 نوفمبر 2014. https://bit.ly/2V5BGyj

وتمتلك روسيا عناصر بشرية مؤهلة للقيام بالعمليات السيبرانية، حيث تعتمد على عدد كبير من القراصنة، سواء المتطوعون، أو الذين يتم توظيفهم لخدمة أغراض عسكرية، وقامت روسيا في عام 2007 بشن حرب سيبرانية شاملة على إستونيا بسبب نقل تمثال يخلد تضحيات جنود روس في الحرب العالمية الثانية[1]، ونتج عنها شل قطاعات البنوك والوزارات وشبكات الاتصالات من خلال هجمات اختراقية سريعة ومدروسة أدت إلى دمار لوجستي كبير، ولم يعد المواطنون قادرين على إجراء معاملاتهم البنكية الإلكترونية التي تتم 97% منها عبر الإنترنت[2]، أو التواصل مع بعضهم بالبريد الإلكتروني لأيام عديدة، وتم تعطيل البنية التحتية للاقتصاد الرقمي الإستوني[3]، وهو ما تكرر أيضًا في أعقاب الحرب الروسية - الجورجية في عام 2008؛ حيث شنت روسيا هجمات سيبرانية من قراصنة لتعطيل شبكة البنية التحتية الجورجية.

4- الوحدة 8200 في إسرائيل:

وحدة تابعة لشعبة الاستخبارات الإسرائيلية "أمان"، تأسست في عام 1952، وأصبحت مسؤولة عن قيادة الحرب السيبرانية في الجيش الإسرائيلي، وتشكل تحالفًا مع وكالة الأمن القومي الأمريكي (NSA) وقيادة الفضاء الإلكتروني (Us Cyber Command)، وتعتبر أهم وأكبر قاعدة تجسس إلكترونية إسرائيلية بالنقب للتنصت على البث الإذاعي والمكالمات الهاتفية، والفاكس، والبريد الإلكتروني في قارات آسيا، وإفريقيا، وأوروبا، ثم أُضيفت إليها مهام الحرب الإلكترونية في وقت لاحق.

1- عادل عبد الصادق، الإرهاب الإلكتروني القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة، مركز الأهرام للدراسات السياسية والاستراتيجية، القاهرة، 2009، ص 216

2- Rebecca Grant, Victory in cyber space, The Air Force Association, October 2007,p 7.

3- عباس بدران، الحرب الإلكترونية.. الاشتباك في عالم المعلومات، مركز دراسات الحكومة الإلكترونية، لبنان، 2010، ص 5.

وقد لعبت هذه الوحدة دورًا رئيسيًّا في ضرب البرنامج النووي الإيراني من خلال تصميم فيروس "ستاكسنت". كما أكد المعلق العسكري الإسرائيلي "عمير رايبوبورت" أن الدور الذي تقوم به "وحدة 8200"، قد جعل إسرائيل ثاني أكبر دولة في مجال التنصت في العالم، بعد الولايات المتحدة، وأشار "رايبوبورت" إلى أن الحواسيب المتطورة التابعة لهذه الوحدة قادرة على رصد الرسائل ذات القيمة الاستخباراتية من خلال معالجة ملايين الاتصالات ومليارات الكلمات[1]

1- صالح النعامي «وحدة 8200».. ذراع التنصت الإلكتروني بإسرائيل، موقع الجزيرة نت، تاريخ مطالعة 11 نوفمبر 2014.

ثالثًا: مفهوم الصراع السيبراني

تعكس أدبيات الصراع ثراءً واضحًا فيما تقدمه من تعريفات لمفهوم الصراع، كما تتعدد أيضًا بؤر الاهتمام، ونقاط التركيز التى يوليها المتخصصون أهمية كبيرة عند تناولهم المفهوم بالدراسة والتحليل. وفي إطار استعراض بعض التعريفات اللغوية التي تقدمها دوائر المعارف والقواميس اللغوية لمفهوم الصراع، فإن دائرة المعارف الأمريكية تعرف الصراع بأنه "حالة من عدم الارتياح أو الضغط النفسى الناتج عن التعارض أو عدم التوافق بين رغبتين أو حاجتين أو أكثر من رغبات الفرد أو حاجاته"[1].

ويذهب قاموس "لونجمان" إلى تعريف مفهوم الصراع بأنه "حالة من الاختلاف أو عدم الاتفاق بين جماعات، أو مبادئ، أو أفكار متعارضة، أو متناقضة". أما قاموس الكتاب العالمى، فإنه يعرف الصراع بأنه "معركة أو قتال Fight، أو بأنه نضال أو كفاح Struggle، خاصة إذا كان الصراع طويلًا أو ممتدًا"[2].

أما في بعده السياسي، فإن الصراع يشير إلى موقف تنافسي خاص، يكون طرفاه أو أطرافه، على دراية بعدم التوافق فى المواقف المستقبلية المحتملة، والتى يكون كل منهما أو منهم، مضطرًا فيها إلى تبنِّي أو اتخاذ موقف لا يتوافق مع المصالح المحتملة للطرف الثاني أو الأطراف الأخرى[3].

وبينما يهتم "لويس كوزر" بالتركيز على الصراع في بعده الاجتماعي، فإن "لورا نادر" تتجه إلى إيضاح البعد الأنثربولوجي في العملية الصراعية؛ فالصراع في بعده الاجتماعي يمثل "نضالًا حول قيم، أو مطالب، أو أوضاع معينة، أو قوة، أو حول

1- The Encyclopedia Americana International Edition, " Danbury , Connecticut: Gerolier Incorporated , 1992: 537.

2- د. منير محمود بدوي، مفهوم الصراع: دراسة فى الأصول النظرية للأسباب والأنواع، مجلة «دراسات مستقبلية»، جامعة أسيوط، العدد الثالث (يوليو 1997)، ص 38-35.

3- Robert North، "Conflict: Political Aspects " in IESS , (1968: 226-232) , P.228

موارد محدودة أو نادرة"، ويكون الهدف هنا متمثلًا "ليس فقط فى كسب القيم المرغوبة، بل أيضًا فى تحييد، أو إلحاق الضرر، أو إزالة المنافسين أو التخلص منهم"[1]. والصراع في مثل هذه المواقف، وكما يرى كوزر، يمكن أن يحدث بين الأفراد، أو بين الجماعات، أو بين الأفراد والجماعات، أو بين الجماعات وبعضها البعض، أو داخل الجماعة أو الجماعات ذاتها. ويفسر "كوزر" ذلك بحقيقة أن الصراع في حد ذاته هو إحدى السمات الأساسية لجوانب الحياة الاجتماعية.

أما فيما يتعلق بالبعد الأنثربولوجى للصراع، فإن الصراع ينشأ أو يحدث نتيجة للتنافس بين طرفين على الأقل. وهنا قد يكون هذا الطرف متمثلًا في فرد، أو أسرة، أو عرق معين، أو مُجتمع كامل. إضافة إلى ذلك، قد يكون طرف الصراع طبقة اجتماعية، أو أفكارًا، أو منظمة سياسية، أو قبيلة، أو دينًا[2].

أحدثت التحولات في مفهوم القوة وتوزيع عناصرها، إلى ظهور مصطلح "الصراع السيبراني"، والذي يشير إلى الطابع التنافسي بين الدول وبعضها البعض، وكذلك بالنسبة للفاعلين من دون الدول، حول الاستحواذ على سبق التقدم التكنولوجي وسرقة الأسرار التقنية والعلمية، وصولًا إلى محاولة السيطرة على شبكة الإنترنت ذاتها. كما أن هذا الصراع السيبراني يتسم بعدم وضوح أطرافه، وأنه غير مكلف ماليًا، ولا يمكن نزع سلاح أطرافه أو تدميرها كما في حالة الحرب التقليدية.

وقد ساهم العلم والتكنولوجيا في تغيير موازين القوى خلال العصور المختلفة، فانتقلت القوة من إسبانيا والبرتغال القوتين العظميين في أوروبا في القرن الخامس عشر الميلادي، إلى هولندا التي أصبحت القوى العظمى في القرن السابع عشر، واحتلت المرتبة الأولى بفضل تطور قوتها البحرية الضاربة، ولكن اندلاع الحروب بينها وبين إنجلترا وفرنسا أضعف من قوة هولندا، وأصبحت بريطانيا وفرنسا من أقوى الدول الأوروبية.

1- Lewis A. Coser, "Conflict: Socail Aspects ", in IESS, (1968:232-236), pp.232-233
2-Laura Nader ,"Conflict: Anthorpological Aspects" , in IESS, (1968 :236-242) , pp236-237.

وفي منتصف القرن العشرين تغير الميزان الدولي من فرنسا وبريطانيا، إلى الولايات المتحدة الأمريكية والاتحاد السوفيتي، وذلك عقب امتلاك الأسلحة النووية، وتطوير صواريخ عابرة للقارات، وبذلك ساهم العلم والتكنولوجيا في تغيير موازين القوى الدولية، وانتقالها من دول إلى أخرى ومن إقليم إلى آخر.

وظل هذا التطور مستمرًا، حيث اعتمدت كل مرحلة من مراحل التطور الإنساني على سلطة أو قوة من طبيعة معينة تتناسب مع متطلبات هذه المرحلة، وقد أثرت هذه السلطة أو القوة بصورة مباشرة أو غير مباشرة في أدوات الصراع بين المُجتمعات وآلياتها، وأفرزت مفردات ومكونات تكاملت معًا لتنتج نظامًا دوليًّا سيطرت مفاهيمه بعض أو كل الوقت.

أما الصراع السيبراني، فيأخذ طابعًا تنافسيًّا حول الاستحواذ على سبق التقدم التكنولوجي وسرقة الأسرار الاقتصادية والعلمية، إلى أن يمتد ذلك الصراع إلى محاولة السيطرة على الإنترنت من خلال السعي للسيطرة على أسماء النطاقات وعناوين المواقع والتحكم بالمعلومات والعمل على اختراق الأمن القومي للدُّول من دون استخدام طائرات أو متفجرات أو حتى انتهاك للحدود السيادية كهجمات قرصنة الكمبيوتر وتدمير المواقع والتجسس، بما يكون لذلك من تأثير على تدمير الاقتصاد والبنية التحتية بنفس القوة التي قد يسببها تفجير تقليدي مدمر[1].

ويتميز الصراع السيبراني بأن به تدميرًا لا تصاحبه دماء أو أشلاء، ويتضمن التجسس والتسلل ثم النسف، لكن لا دخان، ولا أنقاض، ولا غبار، ويتميز أطرافه بعدم الوضوح، وتكون تداعياته خطيرة عن طريق تدمير قواعد البيانات الموجودة على الإنترنت ونسفها أو قصفها بوابل من الفيروسات أو العمل على استخدام

1- عادل عبد الصادق «القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني»، مجلة السياسة الدولية، العدد 188، (مركز الأهرام للدراسات السياسية والاستراتيجية، أبريل 2012)، ص 5.

أسلحة الفضاء الإلكتروني المتعددة للنيل من سلامة المواقع الإلكترونية وقواعد البيانات، وهي أسلحة يسهل الحصول عليها من خلال مواقع الإنترنت وتعلم كيفية استخدامها[1].

ووفقًا لذلك، يمكن القول إن الصراع السيبراني له خصائص تميزه، وهي:

- تنوع الفاعلين الدوليين، وفي بعض الأحيان يكونون مجهولين.

- غير مكلف ماديًّا أو ماليًّا.

- سهولة البداية والانتهاء.

- يحتوي على جانب مادي يتمثل في خضوع الأجهزة والخوادم لسيادة الدولة.

- لا تستطيع الأطراف نزع سلاح الطرف الآخر أو تدميره كليًّا أو احتلال إقليمه.

-إمكانية استخدام الفضاء الإلكتروني في القوة الناعمة أو الصلبة.

- القابلية لتغيير الخصائص مستقبلًا نتيجة التغيرات التكنولوجية السريعة.

ومن هنا أضحى الصراع السيبراني أحد أوجه التفاعلات الدولية الجديدة، شأنه مثل الهجمات السيبرانية والحرب السيبرانية، وهو ما يقابله بالضرورة مفهوم آخر هو "الردع السبيراني"، حتى تتمكن الدول من منع أي فاعل إلكتروني قادر من توظيف الإنترنت بصورة تخدم أهدافه، أو أن يتسبب في إلحاق الأذى بها، وتوصيل رسالة مفادها أن أي هجوم إلكتروني سوف يقابله هجوم مضاد قد يتسبب في خسائر فادحة للخصم.

1- عادل عبد الصادق، الإرهاب الإلكتروني: القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة، مرجع سبق ذكره، ص 4-2.

رابعًا: مفهوم الردع السيبراني

نتيجة للطبيعة الخاصة بالفضاء الإلكتروني، فإن من الصعوبة منع الهجمات السيبرانية بصورة كلية من الأساس، نتيجة للهجمات الصفرية أو الثغرات التي يتم اكتشافها حديثًا أو الفيروسات والأسلحة الإلكترونية التي يتم تطويرها، فضلًا عن صعوبة تعقب مصدر الهجمة ومعرفة الفاعل من الناحية الفنية، ولذا فإن تحقيق الردع بطرقه التقليدية قد لا يتحقق في أفضل الأحوال في الفضاء الإلكتروني، ويثبت نجاحًا فعليًا كما في حالات الردع التقليدي، مثل الردع النووي، وهو ما يهدد بارتفاع حدة الصراعات الإلكترونية إلى أن تصل إلى مرحلة الحرب الإلكترونية الكاملة.

والردع بصفة عامة هو منع الخصم من القيام بفعل عدائي، إما بسبب تخوفه من هجوم مضاد يفوق قدراته الدفاعية، أو ارتفاع تكلفة الهجوم مقارنة بالمكاسب التي يمكن أن يحققها[1]، وهو ما يُعرف بردع الخطر، أي رفع تكلفة الهجوم وتقليل فوائده. ويتطلب تحقيق الردع مكونين رئيسيين، نيات معبر عنها من الطرف الأول برغبته في الدفاع عن مصلحة ما من ناحية، وإدراك الطرف الثاني أن التعارض مع الطرف الأول حول هذه المصلحة سوف يكون مكلفًا له من ناحية أخرى، بصورة تمنعه من اتخاذ أي موقف عدائي نحوه، وهنا يتحقق الهدف الرئيسي من الردع، وهو جعل الطرف الثاني سلبيًّا تجاه الطرف الأول، أي لا يقوم بأخذ أي موقف هجومي نحوه، فهو سعي نحو البقاء على الحالة القائمة Status Quo.

والردع نوعان: ردع بالمنع، أو الردع السلبي، وردع بالانتقام أو الردع الإيجابي. ويحدث الردع بالمنع من خلال تقوية النظم الدفاعية بصورة ترفع تكلفة

1- Clorinda Trujillo, The Limits of Cyberspace Deterrence, The Air War College, Air University, 2014. P 45

هجمات الخصم أكبر من مكاسبه، وغالبًا لا يكون الهدف الرئيسي هنا هو الردع بقدر ما يكون هو الدفاع والتأمين ضد أي عدو محتمل وليس عدوًا محددًا بعينه. وهنا تكون حسابات الخصم بالسالب، أي أن يدرك ارتفاع تكلفة الهجوم مقارنةً بالمكاسب التي يمكن أن يحققها. أما الردع بالانتقام فهو ردع إيجابي يقوم على فكرة العقاب، وفيه يدرك الخصم أن أي هجوم سيتبعه هجوم آخر انتقامي لا يستطيع تفاديه أو تحمله، ويشمل ذلك الإعلان عن المصالح الحيوية واستعراض القوة والتهديد باستخدامها في حالة المساس بها[1].

أما فيما يتعلق بالردع السيبراني، فإنه يعني "قدرة الدولة على تطوير قدرات عسكرية موثوقة ومتبادلة ومتماثلة في الفضاء الإلكتروني، وتكون قادرة على التأثير في قرارات الخصم ومنعه من شن هجمات عسكرية عبر الفضاء الإلكتروني"[2].

ويتشابه الردع السيبراني بصفة عامة مع الردع الإلكتروني في عدة نقاط، منها صعوبة تطبيق القانون في العلاقات العابرة للحدود، حيث يتميز الفضاء الإلكتروني بعدم وجود حدود جغرافية له توضح سيادة الدول عليها. ولمَّا كانت الأسلحة المستخدمة في الفضاء الإلكتروني هي أسلحة غير محددة سلفًا وتخضع للتطور التكنولوجي، فغالبًا ما تظهر الهجمات نتيجة ثغرات تم اكتشافها أو فيروسات تم تطويرها، فيما يُطلق عليه Zero Day Attack، ولهذا يصعب حصر هذه الأسلحة لمنع أو تقنين استخدامها[3].

1-Martin C. Libicki, Cyberdeterrence andCyberwar, Santa Monica, CA: RAND, 2009. P7

2- Jason Rivera, Achieving cyberdetterence and the ability of small states to hold large states at risk, Architectures in Cyberspace, Cycon 2015, NATO Cooperative Cyber Defence Centre Of Excellence, May 2015, p7.

3- Tobias Metzger, Deterrence theory in the cyber-century, Research Division EU/Europe, 02, May 2015

وبناءً على ذلك، فإن ثمة صعوبات عديدة تعترض تحقق الردع في الفضاء الإلكتروني كما في الأسلحة التقليدية وغير التقليدية الأخرى، مثل السلاح النووي والكيماوي. ويُعتبر الردع النووي هو النموذج التقليدي لفهم ودراسة الردع، فالقاعدة الرئيسية تقول: إنه كلما زادت القوة التدميرية للسلاح، قلَّ الميل إلى استخدامه، فالدول التي تمتلك سلاحًا نوويًّا لا تميل إلى استخدامه أو التلويح باستخدامه لتسويه الصراعات بينها، نظرًا للقدرة التدميرية العالية للسلاح، وسهولة تتبُّع الخصم وإلحاق نفس مقدار الأذى به، ومن ثم ترتدع الدول عن استخدامه، ولكن هذا لا ينطبق على الردع في الفضاء الإلكتروني، وذلك لأن البيئة التي يعمل فيها الإنترنت مختلفة تمامًا، **ويتضح ذلك في الآتي:**

1- صعوبة معرفة مصدر الهجمات (الطرف المُعتدي):

لكي يكون الردع ناجحًا، لا بد من توافر ثلاثة عناصر رئيسية، وهي التتبع At-tribution، والتواصل Signaling، والمصداقية Credibility، ويقصد بالتتبع: القدرة على معرفة مصدر الهجمة، من أي تأتي، سواء كان دولة محددة، أو فاعلًا محددًا، في حين يقصد بالتواصل القدرة في الوقت نفسه على إرسال رسالة إلى الجمهور المُستهدف بأن هناك مصلحة معينة يجب عدم التعارض عليها، ويقصد بالمصداقية أنه في حالة الإعلان عن مصدر الهجمة لا بد من أن يكون هناك رصيد كافٍ لدى الجمهور لتصديق هذا الإعلان[1].

وبالتَّطبيق على الفضاء الإلكتروني، يلاحظ أن هناك صعوبة في تحقيق الناصر السابقة، فالبنسبة للتتبع، وعلى الرغم مما وصلت إليه التكنولوجيا من تقدم في عملية التتبع، فإنها تتقدم أيضًا في عمليات التمويه والإخفاء، بصورة تجعل معرفة مصدر الهجمة شبه مستحيل، إلا في حالة الهجمات الصغيرة البسيطة

1 -Clorinda Trujillo, The Limits of Cyberspace Deterrence, The Air War College, Air University, 2014. P 45

التـي يرتكـب أصحابهـا أخطـاء، وليـس في حالـة الهجمـات المعقـدة التـي تقـوم بهـا دول، فمثـلًا الهجمـات الروسـية علـى إسـتونيا عـام 2007، والهجمـات الأمريكيـة الإسـرائيلية علـى المفاعـل النـووي الإيـراني عـام 2010، والهجمـات الكوريـة علـى شـركة سـوني عـام 2015، والـرد الأمريكـي بقطـع الإنترنـت عـن كوريـا لمـدة 10 سـاعات... وجميـع هـذه الهجمـات لـم يتـم تبنِّـي الهجـوم صراحـة مـن قبـل الـدول المعتديـة، بـل إن بعضهـا أنكـر القيـام بذلـك مـن الأسـاس، علـى الرغـم مـن توافـر أدلَّـة مرتبطـة بالظـروف السياسـية، وليـس الفنيـة أو القانونيـة.

أمـا التواصـل، فـلا يتوافـر كذلـك، لأن الفاعـل غيـر معـروف مـن الأسـاس، لكـي يتـم التواصـل معـه، فالمصالـح في الفضـاء الإلكتـروني متشـابكة، وقـد يكـون الفاعـل دولـة، أو فـردًا، أو جماعـة إرهابيـة، أو تنظيمًـا إجراميًّـا، أو غيـره، ومـن ثـم يصعـب إرسـال الرسـالة إلى الجمهـور أو الفاعـل المُسـتهدف.

وبالنسـبة للمصداقيـة، فـإن معظـم حـالات الاختـراق لا يتـم الإعـلان عنهـا مـن ناحيـة، وتنكـر معظـم الـدول الاتهامـات الموجهـة إليهـا بشـن هجمـات إلكترونيـة مـن ناحيـة أخـرى، فالجميـع يتهـم والجميـع ينكـر... فمـن أيـن تـأتي المصداقيـة في الفضـاء الإلكتـروني الـذي صُمِّـم علـى إخفـاء هويـة الطـرف الآخـر.

2- صعوبة وضع الخصم في تهديد حقيقي:

إن الـدول التـي تتعـرَّض لهجمـات إلكترونيـة هـي التـي تسـتطيع أن تُقـدِّر مـدى فداحـة هـذه الهجمـات والخسـائر المترتبـة عليهـا، ومـن ثـم فقـد تقـوم دولـة بشـن هجـوم إلكتـروني انتقامـي علـى دولـة أخـرى بهـدف تحقيـق الـردع بالانتقـام، وأن تسـتطيع إصابـة أهـداف معينـة داخـل الدولـة، لكـن هـذا الجهـوم في تقديـر الدولـة المُعتـدَى عليهـا غيـر مؤثـر، وفي هـذه الحالـة يفشـل تحقيـق الـردع.

وللتوضيح، فعندما قامت كوريا الشمالية بشن هجمات إلكترونية ضد شركة سوني للإنتاج السينمائي في الولايات المتحدة الأمريكية، على خلفية فيلم سينمائي أنتجته شركة "سوني" يسيء لرئيس كوريا الشمالية، فقد ترتَّب على هذه الهجمات تسريب عديد من الإيميلات والأفلام الجديدة على الإنترنت، وكان رد الولايات المتحدة الأمريكية أنها شنَّت هجمات إلكترونية على كوريا الشمالية ترتَّب عليها قطع الإنترنت لمدة 10 ساعات تقريبًا، فهل كان هذا الهجوم مؤثرًا؟

في الحقيقة لكي يمكن الإجابة عن ذلك، لا بد من معرفة الأهداف والخدمات التي يمكن أن تتأثر في دولة مثل كوريا الشمالية بقطع الإنترنت عنها. والإجابة أنه بالفعل لا توجد خدمات حرجة قد تتأثر، ومن ثم فإن الهجوم الأمريكي لم يحقق هدفه، وهو تحقيق الردع بالانتقام، ومن ثم يفشل الردع.

ولكي يمكن أن ينجح الردع بالانتقام من خلال شنِّ هجمات إلكترونية، يجب معرفة الأهداف الحرجة للخصم المُرَاد ردعه، ومصالحه الحقيقية داخل الفضاء الإلكتروني، حتى يكون الهجوم فعالًا، وحتى يحقق الردع هدفه، ولذلك فهناك علاقة طردية بين تعدد الأهداف الإلكترونية التي يمكن إصابتها وبين الردع؛ فكلما تعددت الخدمات والنظم الإلكترونية الحرجة المتصلة عبر الإنترنت، كان الردع ناجزًا وفعالًا، وكلما قلت هذه الخدمات والنظم، قلَّت فاعلية الردع الإلكتروني.

3- صعوبة منع الهجمات الصفرية:

يتميَّز الفضاء الإلكتروني بالتحديث التكنولوجي المستمر، فبصورة يومية يتم اختراع وتطوير فيروسات في معامل خاصة، لم يتم الكشف عنها ولم ترصدها شركات الأمن الإلكتروني، فبعضها يصيب المكون المادي مثل ستاكسنت، وبعضها - وهو كثير – يصيب الجانب البرامجي، وبعضها - وهو أيضًا غير محدود - يركز على المعلومات بهدف السرقة أو التضليل أو التدمير. كما أن

هذه الفيروسات تستغل الثغرات الحديثة التي تظهر في الأنظمة قبل أن يتم تحديثها ومعالجتها، فيما يعرف بالهجمات الصفرية؛ ومن ثم قد تظهر الثغرة اليوم وتستغلها بعض الفواعل لشنِّ هجمة إلكترونية قبل أن يتم اكتشافها ومعالجتها من قبل الأجهزة المختصة، ومن ثم يفشل تحقيق الردع بالمنع، بسبب ثغرات أمنية في أنظمة الدفاع أو بسبب استخدام فيروس جديد تم تطويره.

4- القيود القانونية الخاصة بميثاق الأمم المتحدة:

هناك جانب آخر قد يجعل عملية الردع عبر الفضاء الإلكتروني غير فعَّالة، وهذا الجانب قد يهم القانونيين والسياسيين أكثر من العسكريين، وهو القيود القانونية الخاصة بمبدأ استخدام القوة في العلاقات الدولية وفقًا لميثاق الأمم المتحدة، حيث تنص المادة 2/ 4 من ميثاق الأمم المتحدة على منع استخدام القوة في العلاقات الدولية أو التهديد باستخدامها، إلا بما يتوافق ومقاصد الأمم المتحدة[1]، كما اشترطت المادة 51 من الميثاق ضرورة إبلاغ مجلس الأمن بأية تدابير هجومية سوف تتخذها الدولة في حالة الدفاع عن النفس.

على الرغم من أن الردع السيبراني يعني " قدرة الدولة على تطوير قدرات عسكرية موثوقة ومتبادلة ومتماثلة في الفضاء الإلكتروني، بحيث يمكنها على التأثير في قرارات الخصم ومنعه من شن هجمات عسكرية عبر الفضاء الإلكتروني"؛ فإن هناك صعوبات عديدة تعترض إمكانية تحقيق الردع الكامل في المجال السيبراني، نظرًا لصعوبة معرفة مصدر الهجمات بدقة، وصعوبة وضع الخصم في تهديد حقيقي يردعه، وصعوبة منع الهجمات الصفرية، وعدم وجود أطر قانونية تنظم استخدام القوة السيبرانية في العلاقات الدولية.

1- انظر ميثاق الأمم المتحدة، المادة الثانية، الفقرة الرابعة.

ونظرًا لأن الهجمات السيبرانية هي أحد أشكال استخدام القوة في العلاقات الدولية، أو التهديد باستخدامها، فإنه ينطبق عليها أحكام ميثاق الأمم المتحدة والقيود التي يفرضها، وهو ما قد يكون عائقًا أمام نجاح الردع الإلكتروني وفاعليته.

وينص "دليل تالينTallinn Manual "[1] الخاص بالقواعد المنظمة للحروب الإلكترونية وتنظيم قواعد الاشتباك عبر الإنترنت، على أن العمليات الإلكترونية Cyber Operations التي من شأنها استخدام أو التهديد باستخدام الهجمات السيبرانية ضد إقليم دولة ما أو استقلالية نظام سياسي معين بما يتعارض مع ميثاق الأمم المتحدة، هي أمور غير قانونية[2].

ولما كانت هناك صعوبات فنية بالأساس في تحديد الطرف المُعتدِي، فإن محاسبته قانونيًّا غير واردة، كما أن اتخاذ إجراءات حفظ الأمن والسلم الدولي من قبل مجلس الأمن والأمم المتحدة ضده غير واردة، ومن ثم فالهجمات السيبرانية سوف تستمر بصورة تجعل القول إن الردع السيبراني صعب في أفضل حالته، وربما مستحيل.

وقد دفع ذلك بصورة مباشرة إلى إعادة تعريف الردع والبحث عن تعريف آخر غير تقليدي يتلاءم مع الطبيعة اليسبرانية للعلاقات الدولية اليوم، وهذا قد يتحقق من خلال تبنِّي خطط واستراتيجيات للتعامل مع الهجمات السيبرانية في حالة حدوثها، تشمل التخفيف من حدَّتها، وعدم تأثير البنى التحتية الحرجة والخدمات الرئيسية والمعلومات المهمة التي تشكل ركيزة للأمن القومي للدولة، ويتحقق ذلك من خلال الآتي:

1- هو دليل استرشادي للدول غير مُلزم للأطراف، تم إعداده من قبل لجنة بحلف شمال الأطلسي عام 2013.
2- دليل تالين حول القانون الدولي المنطبق على الحرب السيبرانية – من إعداد اللجنة الدولية للخبراء بدعوة من مركز التميز للدفاع السيبراني التعاوني التابع لحلف شمال الأطلسي (الناتو)، مطابع جامعة كمبريدج 2013، ص 45.

- **إنشاء نظم إنذار مُسبق ومجسَّات إلكترونية** على المرافق والبنية التحتية الحرجة التي يمكن أن تكون عُرضة للهجمات الإلكترونية، بحيث تساعد في اكتشاف الهجمة الإلكترونية فور وقوعها مباشرة، مما يسهل من عملية تفادي المخاطر التي يمكن أن تنجم عنها.

- **تعدُّد مصادر الطاقة داخل الدولة،** فيجب ألا تعتمد الطاقة داخل الدولة على عنصر واحد فقط، فمثلًا إذا تم استهداف شبكات الكهرباء، يجب أن تكون هناك مصادر بديلة - ولو تقليدية - لمنع انقطاع الكهرباء، خاصة عن المؤسسات المهمة والحيوية، كالمستشفيات، والمحلات التجارية الكبرى، والمصانع، وغيرها، بحيث تكون لديها نظم توليد كهرباء بديلة يمكن أن تعمل عليها.

- **إيجاد نظم إلكترونية بديلة للخدمات،** فيجب عدم الاعتماد على نظام إلكتروني واحد، لأنه في حالة تعرضه لهجمة إلكترونية تتوقف الخدمة عنه تمامًا، مثل أنظمة البنوك والأنظمة المالية والخدمات المدنية الحكومية، فهذه الأنظمة يجب أن تتعدد طرق الدخول إليها في حالة استهدافها من خلال أنظمة بديلة تعمل أوقات الطوارئ.

- **إنشاء دعم احتياطي Back Up للبيانات المهمة داخل الدولة،** سواء كانت تخص القطاع الحكومي أو القطاع الخاص، وذلك من خلال تبنِّي استراتيجية شاملة لإنشاء نسخ احتياطية من بيانات مواطني الدولة، بحيث يتم تحديث هذه النسخة بصورة يومية، من خلال مُزامنة Synchronizing البيانات الموجودة بالأنظمة الإلكترونية في مختلفة المؤسسات، مع نظام أرشفة وحفظ البيانات الرئيسي، ومن ثم في حالة تدمير بعض البيانات جراء هجمات إلكترونية، تظل هناك نسخ احتياطية يمكن الرجوع إليها.

- **تشفير البيانات الرئيسية،** وذلك من خلال تشفير البيانات الحرجة والمهمة، مثل البيانات العسكرية، والمُراسلات السرية، فإذا تعرَّضت لإحدى الهجمات

السيبرانية وتمت سرقتها، يصبح من الصعب على الطرف المُعتدِي فهم ما بداخلها، وحتى يكتسب الطرف المُعتدَى عليه بعض الوقت من أجل المناورة، إما باكتشاف هذا الطرف ومفاوضته، أو الإعلان المُسبق عنها.

ومن ثم يجب على الدولة أن تعمل وفق استراتيجية شاملة للفضاء الإلكتروني تشمل المؤسسات الحكومية والعسكرية، إلى جانب القطاع الخاص والمُجتمع المدني والأفراد، وتقوم بالتوعية الكاملة بالتهديدات المحتملة المقبلة من الفضاء الإلكتروني وكيفية التعامل معها، وإنشاء جهات مختصة قادرة على التعامل مع هذه التهديدات واكتشافها في وقت مبكر.

ليس هذا فحسب، بل إن الدول يجب عليها تطبيق مفهوم الردع بالمنع، من خلال إنشاء نظم إلكترونية، مثل الدروع السيبرانية Cyber Shield، والشبكات المغلقة Intranet، والقيام بعمليات اختبار دائمة للشبكات Cyber Drill بهدف معرفة مواطن الضعف فيها والعمل على علاجها. وعلى الدول أيضًا تطبيق مفهوم الردع بالانتقام، من خلال تبنِّي الموهوبين من الطلاب في مجال الكمبيوتر، وإنشاء قسم خاص في المؤسسات العسكرية للقراصنة الإلكترونيين، وشنِّ هجمات إلكترونية على المشكوك في قيامهم بمهاجمة أنظمة ومؤسسات الدولة.

وبالإضافة إلى ذلك، يجب تطبيق مفهوم "الردع بالاستيعاب" من خلال زيادة مرونة أنظمة الدولة في التعامل مع الهجمات السيبرانية، وتبنِّي خطط بديلة دائمًا، وأنظمة أخرى يمكنها أن تحل محل الأنظمة التي تتعرض لهجمات إلكترونية أو تخرج من الخدمة، واتباع مبدأ المصارحة والشفافية في المعلومات، حتى وإن تمت سرقة معلومات وتسريبها، فإنها في النهاية تعكس توجه الدولة الحقيقي، ولا تمثل قيمة مضافة في عالم السياسية.

خامسًا: مفهوم الدفاع السيبراني

في ضوء التطور التكنولوجي المُتسارع، وتنامي دور الفاعلين من النشطاء والجيوش الإلكترونية والفواعل من دون الدول في المجال السيبراني، زادت التهديدات الإلكترونية، بصورة شملت ليس فقط المواقع والخدمات المدنية، ولكن أيضًا البيانات والمنشآت العسكرية، بالإضافة إلى البنية التحتية الحرجة كالمفاعلات النووية، وهو تطور يفرض تحديات حقيقية أمام حفظ الأمن القومي للدُّول.

ويُقصد بالدفاع السيبراني "مجموعة القدرات النظامية التي تمتلكها القوات المسلحة للحماية من تأثيرات الهجمات السيبرانية، والتخفيف من حدتها والتعافي منها بسرعة"[1]. وقد عرَّفت العقيدة الفرنسية الدفاع السيبراني بأنه: "مجموعة الوسائل الفنية وغير الفنية التي تسمح للدولة بالدفاع في الفضاء الإلكتروني عن نظم المعلومات الحرجة"[2]، وفي الاستراتيجية النمساوية، فإن مصطلح الدفاع السيبراني يشير إلى "جميع التدابير اللازمة للدفاع عن الفضاء الإلكتروني بالوسائل المناسبة لتحقيق الأهداف العسكرية الاستراتيجية"[3]، ويعرفه البرلمان الأوروبي بأنه "عملية تطبيق الإجراءات الأمنية من أجل الحماية من الهجمات السيبرانية، والتعامل معها، بما تستهدف تأمين البنية التحتية لنظم الاتصالات والسيطرة"[4].

1- Habes B. Godwin III (et al.) (eds.), Critical Terminology Foundations 2: Russia – US Bilateral on Cybersecurity, East-West Institute, Policy Report no. 2, 2014, accessible at: https://dl.dropboxusercontent.com/u/164629289/terminology2.pdf

2- France's Strategy 2011, Information Systems and Defence, Agence nationale de la sécurité des systèmes d›information (ANSSI), accessible at: https://goo.gl/MXfmXx(Last accessed: July 26, 2017).

3- Austrian Cyber Security Strategy 2013,Federal Chancellery of the Republic of Austria, 2013, accessible at: https://bit.ly/2RkOTV3 (Last accessed: July 26, 2017).

4- Carmen- Cristina, Cyber defence in the EU Preparing for cyber warfare?, European Parliamentary Research Service, October 2014, accessible at: https://goo.gl/ceKME2(Last accessed: July 27, 2017).

وفي الاستراتيجية العسكرية البلجيكية، فإن الدفاع السيبراني هو "تطبيق تدابير وقائية فعالة للحصول على مستوى مناسب من الأمن السيبراني، وتقليل المخاطر الأمنية إلى مستوى مقبول"[1].

ويُلاحظ أن جميع التعريفات السابقة تطرقت إلى الدفاع السيبراني بمفهومه السلبي، والذي يعني القدرة على استقبال الهجمة الإلكترونية، وتلافي آثارها سريعًا دون الإضرار بالبنية التحتية والأهداف الاستراتيجية للدولة؛ أما التعريف البلجيكي فقد أضاف بعدًا جديدًا، وهو الدفاع السيبراني الوقائي أو الإيجابي، والذي يعني منع الهجمة قبل حدوثها، سواء من خلال اتخاذ تدابير وقائية، أو هجمات إلكترونية استباقية.

ومن مجمل التعريفات السابقة، يمكن تعريف الدفاع السيبراني الوقائي بأنه: "وسيلة لتحقيق الأمن السيبراني من خلال استخدام آليات رصد الهجمات السيبرانية وتحليلها وتحديد مصدرها والتخفيف من حدة آثارها على نظم الاتصالات والشبكات والبنية التحتية، وذلك في وقتها الحقيقي، مع توافر القدرات الهجومية لتعقب الكيانات وتدمير الشبكات، التي انطلق منها هذا التهديد"[2].

ويختلف الدفاع الوقائي عن نظيره التقليدي في عنصرين رئيسيين، هما الاكتشاف المبكر للهجمات الإلكترونية، والتعامل معها في حالة حدوثها؛ فبينما يعمل الدفاع التقليدي كدرع داخلية للتخفيف من حدة الهجمات والتعافي السريع منها، يعمل الدفاع الوقائي كرمح استباقي لإعاقة الخصم عن تنفيذ الهجمة الإلكترونية، **ويتحقق الدفاع السيبراني الوقائي من خلال ثلاثة أساليب رئيسية، وهي:**

1- Cyber Definitions, NATO Cooperative Cyber Defence Centre of Excellence, accessible at: https://ccdcoe.org/cyber-definitions.html(Last accessed: July 28, 2017).
2- Robert S. Dewar, The "Triptych of Cyber Security": A Classification of Active Cyber Defence, NATO Cooperative Cyber Defence Centre of Excellence, 2014, (p. 10), accessible at: https://bit.ly/1k8gBzZ (Last accessed: July 29, 2017).

1- الكشف المبكر للهجمات في وقتها الحقيقي:

يتم تحقيق هذا الأمر من خلال استخدام مجسَّات على الشبكات والبرامج والتَّطبيقات، بالإضافة إلى توظيف المعلومات الاستخباراتية لرصد أي نشاط غير طبيعي قد يُصنف على أنه هجمة إلكترونية، وبداية مواجهتها واحتوائها قبل أن تبدأ نشاطها في الشبكة أو النظم المستهدفة.

2- الهجوم السيبراني الاستباقي:

يتم ذلك من خلال استخدام ونشر الديدان البيضاء White Worms، وهي برامج قادرة على اكتشاف التَّطبيقات الضارة وتدميرها قبل توظيفها في إطلاق هجمة إلكترونية محتملة. كما تقوم أيضًا بتدمير أدوات وبرمجيات القراصنة، وهو ما يساعد في إحباط مخطط الهجمة نفسها، وليس التصدي لها فحسب[1]، كما يشمل أيضًا مهاجمة الخصم، فما أن يتم تحديد هوية ومصدر الهجمة، حتى يمكن إطلاق هجمة إلكترونية مضادة فيما يعرف بالاختراق العكسي (Hack-Back).

أضحت العديد من العقائد العسكرية للدول تعتمد مفهوم "الدفاع الإلكتروني" وفق رؤيتها لأمنها الوطني، ويُقصد به بوجه عام "مجموعة القدرات النظامية التي تمتلكها القوات المسلحة للحماية من تأثيرات الهجمات السيبرانية، والتخفيف من حدتها والتعافي منها بسرعة"، بما يشمله ذلك من الكشف المبكر عن الهجمات في وقتها الحقيقي، وإمكانية القيام بهجوم إلكتروني استباقي، واتباع وسائل مختلفة للتضليل والإخفاء والخداع في المجال السيبراني.

3- التضليل والإخفاء والخداع:

يتم عن طريق إخفاء هويات الأهداف الاستراتيجية للدولة على الإنترنت، وتضليل الخصم أثناء محاولة الوصول إليها أو اختراقها، من خلال أدوات التمويه

1- Ibid., p. 10.

والخداع وتغيير ملامح الأهداف الاستراتيجية للدولة، بما يساعد على تضليل الخصم وتشتيت الانتباه عن الهدف الرئيسي.

وتتمحور أهداف الدفاع السيبراني في الحفاظ على مقدرات الأمن القومي التكنولوجي للدولة، من خطوط اتصالات، وشبكات كمبيوتر، وبنية تحتية، سواء مدنية، أو عسكرية، فضلًا عن تأمين البيانات الحيوية، بما يساهم في النهاية في تحقيق الأمن السيبراني للدولة والدفاع عن مصالحها في الفضاء الإلكتروني وتدعيم قدراتها في مجال الحروب الإلكترونية، وردع أي محاولة لزعزعة استقرارها عبر الإنترنت، **ولذلك يمكن تحديد أهداف الدفاع السيبراني في التالي:**

1- حماية الأهداف العسكرية:

تشمل هذه الأهداف نظم الإدارة والمراقبة ونظم التحكم والسيطرة ونظم توجيه الأسلحة وقطاع الاتصالات الحربية والأسلحة آلية القيادة، مثل الطائرات من دون طيار، فضلًا عن تأمين المنشآت العسكرية، مثل محطات الطاقة النووية من أي اختراق إلكتروني.

2- حماية البيانات العسكرية:

تشمل المعلومات حول أفراد القوات المسلحة كالأسماء، والرتب، والمرتبات، والوظائف داخل الجيش، وأماكن الإقامة الشخصية، فضلًا عن خطط التسليح وتصميمات الأسلحة، وخرائط انتشار القوات وتوزيع الأسلحة وغيرها من المعلومات السرية.

3- حماية البنية التحتية الحرجة:

تشمل على سبيل المثال قطاعات الاتصالات والمواصلات، ومحطات الطاقة، ونظم إدارة المرور، وقواعد البيانات الحكومية، وخدمات الحكومات الذَّكيَّة، والبنوك والمؤسسات المالية والمصرفية.

4- دعم وحدات الحرب السيبرانية:

هي تلك الوحدات الخاصة بإدارة الحروب السيبرانية للدولة، حيث تكون مهمة الدفاع السيبراني تأمين الخطوط خلف هذه الوحدات، بما يحمي أهداف الدولة الاستراتيجية في حالة شنِّ هجوم إلكتروني مضاد عليها، وتوفير غطاء إلكتروني للوحدات المقاتلة بهدف التمويه والخداع وصعوبة تعقب مصدر الهجمة.

5- تحقيق الردع السيبراني:

يتم ذلك من خلال رفع تكلفة الهجوم السيبراني على الدولة المُعادية، عبر إنشاء نظم دفاع إلكترونية صعبة الاختراق تحتاج إلى وقت وجهد كبير لاختراقها، مع تطوير قدرات تتبع الهجمات السيبرانية واكتشاف مصدرها، بما يؤدي في النهاية إلى التأثير على قرارات الخصم وردعه من شنِّ هجمات إلكترونية على الدولة في النهاية.

6- تحقيق الأمن السيبراني:

إن الهدف الرئيسي من الدفاع السيبراني، هو تحقيق الأمن السيبراني داخل الدولة بصفة عامة، أي ضمان سلامة واستقرار الشبكات والأجهزة، واستمرار تقديم الخدمات الإلكترونية.

ووفقًا لدراسة مسحية أجراها مكتب الأمم المتحدة لشؤون نزع السلاح في عام 2012 على الدول الأعضاء في منظمة الأمم المتحدة،والبالغ عددها نحو 193 دولة، حول مؤسسات الدفاع السيبراني، فقد وُجد أن من بين هذه الدول 114 دولة لديها برامج وطنية للأمن السيبراني، وأن 74 دولة منها أولت مهمة تحقيق الأمن السيبراني للقوات المسلحة، بينما قامت 67 دولة بإناطة مهمة الأمن السيبراني لمؤسسات مدنية لديها[1].

1- -Carmen- Cristina, Cyber defence in the EU Preparing for cyber warfare?, European Parliamenta-

وبصورة عامة، فإن مهمة تحقيق الدفاع السيبراني تقع على عاتق عدد من المؤسسات، سواء العسكرية، أو المدنية، **وذلك على النحو التالي:**

1- الجيوش الإلكترونية:

اتَّجه كثير من الدول حول العالم – كما سبق شرحه سابقًا – إلى إنشاء جيوش إلكترونية وفرق للعمليات عبر الفضاء الإلكتروني داخل صفوف قواتها المسلحة، تتكون من قراصنة معلومات مهمتهم اختراق شبكات الكمبيوتر الخاصة بالخصوم، ونشر برامج التجسس والمراقبة، وتنفيذ المهمات العسكرية التي تطلب منها، كتعطيل أحد البرامج العسكرية للخصم، أو السيطرة على إحدى الشبكات، أو تدمير بعض الخدمات الإلكترونية، فضلًا عن الدفاع عن الشبكات القومية وحمايتها من أي محولة اختراق.

2- فرق الاستجابة الفورية للطوارئ Computer Emergency Response Team:

هي فرق مدنية، تكون مهمتها التحقيق في الأدلَّة الجنائية الرقمية، ومحاولة تتبُّع مصدر الهجمات والمتورطين فيها[1]، وعادة ما

يوجد بالدولة أكثر من فريق استجابة للطوارئ، يتبع بعضها الوزارات، مثل وزارة الاتصالات، ويتبع البعض الآخر الشركات الكبرى، سواء كانت حكومية، أو غير حكومية، كشركات النفط، والطاقة، والاتصالات.

ry Research Service, October 2014, Accessed July 27, 2017 on, https://bit.ly/2mBrHCj

1- CERT (Computer Emergency Readiness Team), Techtarget, accessed 10 August 2017, on: https://bit.ly/2R8M2P7

3- كبرى شركات الاتصالات:

تمثل هذه الشركات أيضًا أحد خطوط الدفاع السيبراني للدولة، وذلك بسبب امتلاكها لقواعد بيانات خاصة بعدد كبير من المستخدمين داخل الدولة، كما تقع عليها مسؤولية تأمين جميع اتصالات الأفراد بالدولة، وضمان الحفاظ على سرِّيتهم وخصوصياتهم دون أن تتعرَّض للاختراق أو التسريب.

4 - القوات المسلحة التقليدية:

قد تشارك بعض فرق القوات المسلحة التقليدية أيضًا في عمليات الدفاع السيبراني، حيث تستدعي بعض العمليات الإلكترونية التدخل العسكري التقليدي من قبل القوات المسلحة، لتدمير خطوط اتصالات أو مراكز إدارة عمليات قرصنة تابعة للخصم، أو تدمير أسلحة خرجت عن السيطرة بسبب اختراقها.

خاتمة

سوف تشهد السنوات القليلة المقبلة تغيُّرًا جذريًّا في أنماط حياة الأفراد، وطرق إدارة الدول والمؤسسات، وأشكال الحروب والصراعات، مدفوعة في ذلك بتقنيات أكثر ذكاءً ودقَّةً وكفاءةً في مجملها من قدرات الإنسان، تتمثل في نظم الذَّكاء الاصطناعي، والطابعات ثُلاثيَّة، ورُباعية الأبعاد، وتقنيات إنترنت الأشياء، والسيارات ذاتية القيادة، والدرونز، والحاسبات الكمومية، ونظم "البلوك تشين" القادرة على إدارة جميع المعاملات البشرية... وحينها تكتسح "الثَّورة الذَّكيَّة" كل المفاهيم والطرق التقليدية التي عرفتها البشرية منذ بدء الخليقة.

وربما قد يعجز العالم عن مواجهة التسونامي التكنولوجي الذي بدأ في التحرُّك بالفعل، ليظهر عصر جديد من البشرية يُصبح الإنسان فيه هو العبد، بينما الآلة هي السيد، وهو ما يتطلب وجود رؤية شاملة لما ستكون عليه حياة الأفراد في السنوات المقبلة، وكيف يمكن التعامل مع التحديات والتهديدات التي تطرحها الثَّورة الذَّكيَّة، وتحديد الاحتياجات الجديدة للأفراد التي سوف تخلقها هذه الثَّورة، والبحث عن موارد جديدة لإشباع هذه الحاجات، حتى لا يقع الإنسان ضحية إنجازاته التكنولوجية.

وقد حاول هذا الكتاب خلال أربعة فصول تقديم القوى التكنولوجية المُحرِّكة للثورة الذَّكيَّة التي سوف تؤثر على حياة البشرية في المستقبل القريب، لتنقلها إلى مرحلة "مُجتمع ما بعد المعلومات"، أو "المُجتمع الخامس" الذي يأتي بعد أربعة مُجتمعات هي الصيد، والزراعة، والصناعة، والمعلومات، لينهي بذلك مرحلة من الحياة الإنسانية، ويعلن تدشين مرحلة جديدة، قد تهيمن فيها العقول الصِّناعيَّة على العقول البشرية، وتتحكَّم في حياة الأفراد مجموعة خوارزميات تُرتِّب لهم أولوياتهم، وأفكارهم، واحتياجاتهم، وتتَّخذ بدلًا منهم قراراتهم، وتُدير شؤون حياتهم اليومية، مثل المساعدات الصوتية الذَّكيَّة، وتقنيات الواقع المُعزَّز، وإنترنت الأشياء، وتتولىَّ المركبات ذاتية التحكُّم شؤون تحرُّكاتهم وتنقُّلاتهم، وتقوم الطابعات ثُلاثيَّة الأبعاد بطباعة أطعمتهم الغذائية، وأعضائهم البشرية، ومتطلبات حياتهم اليومية، لتصبح حياة الأفراد عبارة عن مشاهدة أحد أفلام الخيال العلمي.

ومع توجُّه الدول لتبنِّي نماذج المدن الذَّكيَّة التي تعتمد بصورة رئيسية على تكنولوجيا المعلومات والاتصالات لإدارة جميع متطلبات الحياة اليومية فيها، واعتماد النظم المالية والمصرفية والإدارية على الانترنت، وانتشار أجهزة

انترنت الأشياء والذَّكاء الاصطناعي في كل مكان، تُصبح الدول والأفراد أكثر عُرضة للاختراق، وتُصبح جميع الخدمات الحكومية أكثر عُرضة للتوقف المفاجئ من خلال هجمات القراصنة، وتصبح قواعد البيانات والخطط والاستراتيجيات والوثائق والمعلومات السرية عُرضة للتلاعب بها وتسريبها، وتُصبح الأسلحة والأدوات العسكرية قليلة التكلفة وسهلة التصنيع وشديدة التدمير، وهي عبارة عن فيروسات كمبيوتر، وتزداد احتمالية نشوب صراعات سيبرانية بين الدول لا يمكن احتواؤها، حتى تتطوَّر وتصل إلى مرحلة الحرب السيبرانية الشاملة.

وسوف يؤثر ذلك بصورة كبيرة على إعادة صياغة كثير من المفاهيم الأمنية التقليدية، مثل القوة، والحرب، والصراع، والدفاع، والردع؛ حيث تتغيَّر مصادر تهديد الأمن القومي للدُّول، لتُصبح الهجمات السيبرانية أحد أخطر مصادر التهديد، وتحل الأسلحة السيبرانية محل كثير من الأسلحة التقليدية، وتتجه الدول نحو إنشاء قوات عسكرية سيبرانية وأحلاف عسكرية سيبرانية مهمتها الدفاع عن مصالح الدولة عبر الفضاء السيبراني، مما قد يدفع المُجتمع الدولي قريبًا لتبنِّي مُعاهدة دولية تحافظ على الطبيعة السلمية والمدنية للإنترنت الذي يُمثِّل العمود الفقري لجميع التطورات التكنولوجية.

عن المؤلف:
إيهاب خليفة

- رئيس وحدة التطورات التكنولوجية بمركز المستقبل للأبحاث والدراسات المتقدمة - أبوظبي، وباحث سابق بمجلس الوزراء المصري، وباحث دكتوراه متخصص في مجال إدارة المدن الذكية.

- مؤلف كتاب "القوة الإلكترونية: كيف يمكن للدول أن تدير شؤونها في عصر الانترنت" الحاصل على جائزة أفضل كتاب في مجال العلوم الرقمية في عام 2018 من معرض القاهرة الدولي للكتاب، ومؤلف كتاب "حروب مواقع التواصل الاجتماعي" الصادر في عام 2016.

- تخرج في كلية الاقتصاد والعلوم السياسية جامعة القاهرة عام 2009، بتقدير جيد جداً مع مرتبة الشرف، وله العديد من الأبحاث العلمية المنشورة باللغة العربية والإنجليزية حول الحروب السيبرانية والتداعيات الناجمة عن تزايد الاعتماد على التقنيات الذكية في الحياة البشرية، ومصادر تهديد الأمن القومي.

للتواصل: ehabakhalifa@gmail.com